Marie LERIN

MST Télécoms
2ème année

MISE EN PLACE DU SITE DE BACK UP INTERNET

Du 04 Avril au 27 Juin 2005
Suivi par : M. Robert Forêt

BANQUE POPULAIRE
BANQUE POPULAIRE LORRAINE CHAMPAGNE

paul verlaine
université - metz

Je remercie Monsieur FORET de m'avoir permis de réaliser mon stage au sein du Centre Informatique de Metz de la Banque Populaire Lorraine-Champagne.

Je tiens également à remercier tout le personnel du Département Systèmes et Réseaux pour l'aide qu'ils m'ont apporté durant mon stage et pour le matériel mis à ma disposition.

Sommaire

Introduction ……... 4

Présentation de l'entreprise ……... 5

Le Groupe Banque Populaire

Quelques chiffres

Implantations internationales

Les Banques Populaires

La Banque Populaire Lorraine-Champagne

Le Centre Informatique de Metz

Présentation du stage ……... 16

Découverte de l'infrastructure ……. 17

Missions …….. 28

Gestion réseaux

Automates

Messagerie

Optimisation du site central

Fiabilisation de l'accès Internet

Conclusion …….. 56

Annexes ……... 57

Introduction

La formation en deuxième année de MST Télécommunications à l'Université Paul Verlaine de Metz se termine par un stage pratique en entreprise. Le stage que j'ai effectué au Centre Informatique de Metz (CIM) de la Banque Populaire Lorraine-Champagne avait pour objet principal la mise en place d'un site de back-up Internet et l'optimisation du site central. Il a eu lieu de d'Avril à Juin 2005.

Les réseaux d'entreprises représentent une petite partie du programme d'enseignement de la Maîtrise, c'est pour cette raison que j'ai choisi d'approfondir ce domaine dans le cadre de mon stage.

Dans ce rapport, je vais tout d'abord présenter la Banque Populaire Lorraine-Champagne, puis présenter en détails l'objet de mon stage ainsi que le matériel sur lequel j'ai travaillé. Enfin, je ferai le point sur cette expérience et les perspectives d'avenir.

Présentation de l'entreprise

1- Le Groupe Banque Populaire

Profil :

Le Groupe Banque Populaire associe les atouts de la culture coopérative des Banques Populaires, banques de proximité et ceux de l'approche globale et internationale des métiers de financement, d'investissement et de service de Natexis Banques Populaires, son véhicule coté.

Son organisation en trois dimensions, coopérative, fédérale et capitalistique, le distingue au sein du monde bancaire et lui confère un modèle de développement original.

Les 22 Banques Populaires, de statut coopératif, sont les maisons mères du Groupe et actionnaires de la Banque Fédérale des Banques Populaires. Autonomes, elles exercent tous les métiers de la bancassurance dans une relation de proximité avec leurs clientèles. Elles rassemblent 20 Banques Populaires régionales, la CASDEN Banque Populaire et, depuis fin janvier 2003, le Crédit Coopératif.

La Banque Fédérale des Banques Populaires, dimension fédérale, réunit les fonctions d'organe central du Groupe Banque Populaire et de holding de Natexis Banques Populaires. Elle assure à la fois le rôle de contrôle, de coordination et d'animation de l'ensemble du Groupe.

Natexis Banques Populaires, coté sur l'Eurolist Paris, est présent dans les métiers de financement, d'investissement et de services. Sa palette de prestations aux entreprises et d'implantations à l'étranger a été enrichie par l'acquisition de Coface en 2002.

Valeurs :

Le Groupe Banque Populaire reconnaît comme principes d'action trois valeurs fondamentales :

L'AUDACE **:** Fondé par des entrepreneurs au service des entrepreneurs, le Groupe Banque Populaire cultive l'envie d'entreprendre. Il aime mettre en mouvement l'énergie créatrice de ses clients et collaborateurs. Il respecte le courage, la ténacité et l'enthousiasme des porteurs de projets professionnels ou de projets de vie. L'audace d'entreprendre implique l'optimisme. Elle fait progresser constamment.

LA COOPÉRATION : Son histoire, son fonctionnement, son expérience quotidienne, illustrent l'aptitude du Groupe Banque Populaire à faire vivre la coopération. La coopération, c'est agir ensemble pour gagner ensemble, en assumant toutes ses responsabilités à l'égard du partenaire et de la société. Elle implique la confiance réciproque. Elle n'a de sens que dans la durée. Elle résiste à la pression du court terme. Acteurs majeurs de la vie économique, solidaires de leur région, les Banques Populaires sont également solidaires entre elles. Cette solidarité est le ciment du Groupe Banque Populaire. Elle unit l'ensemble de ses composantes. Elle l'ouvre sur d'autres partenaires.

L'HOMME : Le Groupe Banque Populaire s'est construit sur le respect des parcours de vie, des sensibilités, des attentes, des particularités de ses clients et partenaires. Chaque porteur de projet est unique : pour se mettre en mouvement avec les meilleures chances de succès vers son objectif, il a besoin d'être écouté, d'être informé de façon claire et transparente, d'être compris. Placer l'homme au coeur des préoccupations donne tout son sens et toute sa force à la relation bancaire.

2- Quelques chiffres

Banques Populaires ……..…….. 22

Sociétés de Caution Mutuelle ……..…… 94

Agences …….. 2 692

Clients ……. 6 600 000

Collaborateurs …….. 44 509

Sociétaires ……... 2 770 000

Implantations internationales …… 116

Résultats :

(en millions d'euros)

Produit net bancaire ……...…… 7 640

Résultat brut d'exploitation …… 2 545

Capacité bénéficiaire ……..…… 1 174

Résultat net part du groupe …… 1 059

(en milliards d'euros)

Fonds propres totaux …… 17,2

Ratio Tier one …… 9,1 %

Encours de crédits …….. 121,3

Epargne bilantielle ……... 94,8

Epargne financière ……... 97,4

3- Implantations internationales

4- Les Banques Populaires

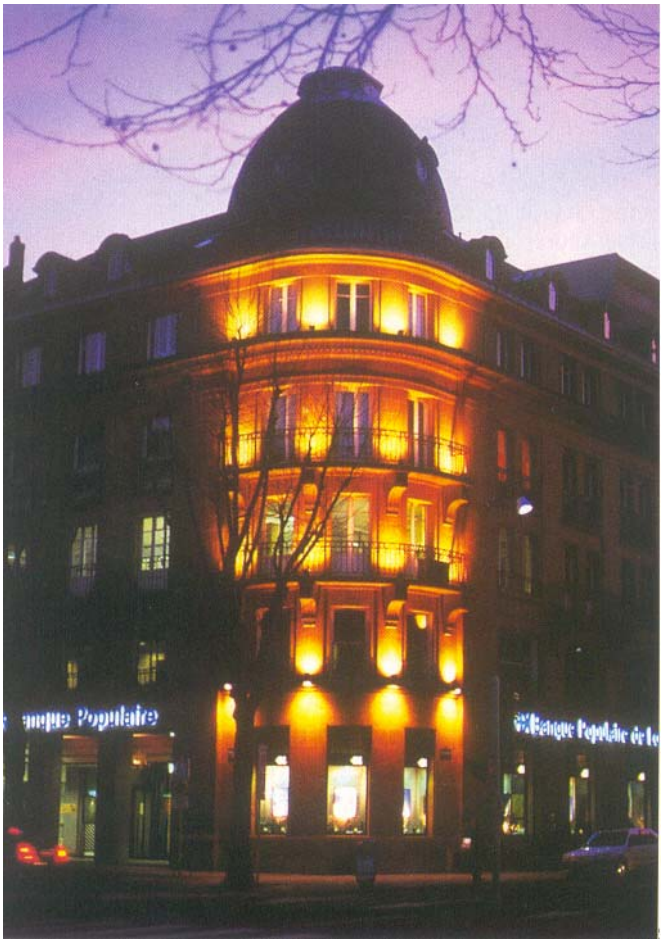
BANQUES COOPÉRATIVES : Sociétés anonymes coopératives, les Banques Populaires sont les maisons mères du Groupe. Elles regroupent :
- 20 Banques Populaires régionales,
- la CASDEN Banque Populaire qui s'adresse aux personnels de l'Education Nationale, de la Recherche et de la Culture,
- le Crédit Coopératif, acteur majeur du domaine de l'économie sociale.

Elles appartiennent à plus de 2,7 millions de sociétaires et incarnent l'esprit coopératif au quotidien.

BANQUES RÉGIONALES : Banques de proximité, proches de leurs clients, de leurs sociétaires et des multiples acteurs de l'économie régionale, elles sont pleinement engagées dans la réussite économique et humaine du territoire sur lequel elles sont implantées. Toutes entretiennent des relations étroites avec les organisations socioprofessionnelles locales et les organismes consulaires où siègent bon nombre de leurs administrateurs. Elles sont animées par deux dirigeants :
- le Président, sociétaire, souvent chef d'entreprise local, élu par ses pairs au sein du Conseil d'Administration de la Banque.
- le Directeur Général, banquier, dont la nomination par le Conseil d'Administration est agréée par la Banque Fédérale des Banques Populaires.

BANQUES DE PROXIMITÉ : Première des proximités, le réseau des Banques Populaires ne cesse de s'agrandir. Il compte 2 692 agences depuis l'arrivée du Crédit Coopératif début 2003. Mais cette proximité se décline aussi à travers tous les canaux de relations à distance : centres d'appels, banque en ligne, télétransmission.

5- La Banque Populaire Lorraine-Champagne



Née en mai 2002 de la fusion de deux banques en pleine évolution (la Banque Populaire de Lorraine et la Banque Populaire de Champagne) la Banque Populaire Lorraine-Champagne a pour objectif d'asseoir son emprise sur le marché et d'accroître son développement. L'entreprise dispose d'une puissance humaine, économique et financière accrue pour accompagner les enjeux économiques de demain.

Présente dans les 7 départements de Lorraine et de Champagne, la Banque Populaire participe activement à l'élaboration de nombreux projets à travers le financement d'investissements d'entreprises, de projets immobiliers et de prêts personnels.

La Banque Populaire Lorraine-Champagne compte parmi les acteurs économiques majeurs de la région et connaît de ce fait particulièrement bien les préoccupations de ses interlocuteurs. Ouverte sur l'Europe, des partenariats de qualité lui permettent de répondre aux demandes d'une clientèle étrangère désireuse de s'installer en France. Elle est aujourd'hui le plus important réseau bancaire régional en terme de parts de marché, et le nombre de clients, particuliers et professionnels, qui lui accordent chaque jour leur confiance, ne cesse de croître. La Banque Populaire Lorraine-Champagne attache une attention particulière aux besoins et aux attentes de ses clients. Largement investie dans les nouvelles techniques de communication et d'information, elle allie judicieusement proximité et technologie. Cette banque "multi-canal", offre à ses clients les avantages d'un contact personnalisé dans une agence de proximité et la commodité des autres modes d'accès de la banque : automates, minitel, Internet, téléphone.

La BPLC en chiffres :

Agences ……... 130

Collaborateurs …….. 1 400

Sociétaires …… 135 000

Départements …….. 7

Fonds propres ……... 592 M€

Produit net bancaire …….. 272 M€

Résultat net ……. 31 M€

6- Le Centre Informatique de Metz

Outre sa position de banque régionale appartenant au groupe des Banques Populaires, la BPLC dispose d'un service informatique d'envergure qui gère les applications bancaires ainsi que le réseau informatique. La BPLC propose également des prestations d'hébergement, de développement de sites Web et d'accès à Internet à ses clients. Ce service informatique est appelé CIM (Centre Informatique de Metz), il est situé au siège de la banque à Metz-Gare, il couvre toutes les agences dans les sept départements de la BPLC.

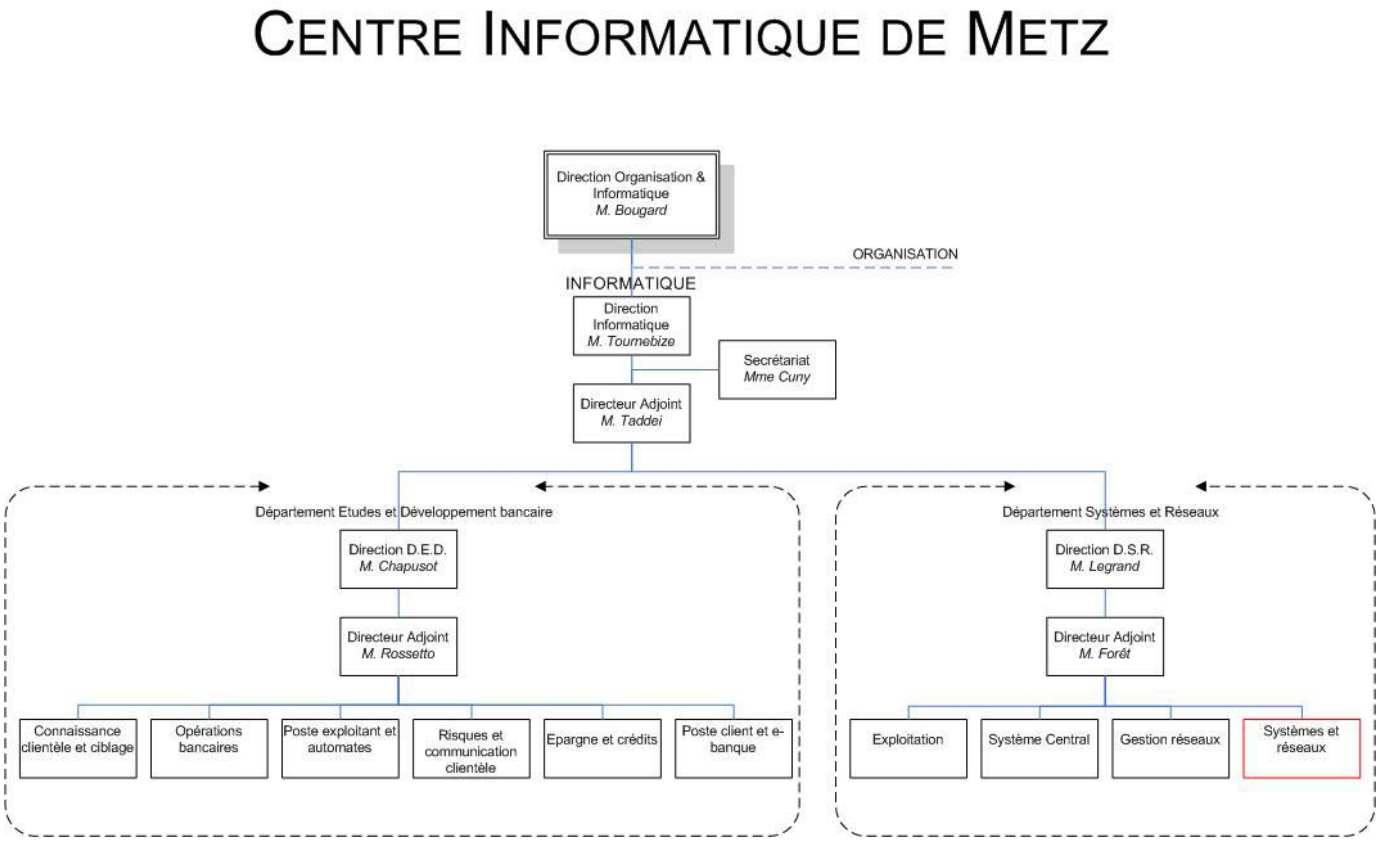
Il n'en a pas toujours été ainsi, l'infrastructure informatique de la Banque Populaire de Lorraine a su traverser toutes les étapes du développement de l'informatique. Le service informatique a été créé en 1956. Par son savoir-faire et ses réalisations, il a rapidement aquis une notoriété dépassant le cadre de la région. Les banques Populaires des régions avoisinantes (Nord, Champagne, Côte d'Or, Jura) confrontées à un problème de développement, ont souhaité bénéficier de l'avance technologique de la Banque Populaire de Lorraine et ont proposé un regroupement des traitements informatiques.

C'est en 1975, que la banque a commencé à utiliser des ordinateurs pour ses opérations. Ils disposaient de consoles financières IBM aux guichets, avec un affichage de 8 lignes x 40 caractères afin de permettre aux banquiers de saisir leurs opérations. A cette époque les entrées correspondaient à des entrées comptables brutes et bien souvent les guichetiers devaient apprendre par cœur toutes les instructions. Par la suite, dans le courant des années 1980, on a commencé à développer des consoles passives dans les agences bancaires, qui permettaient au personnel des agences de saisir leurs opérations. Les capacités des machines étaient alors extraordinaires pour l'époque : elles disposaient de 10 Mo de mémoire et d'un écran de 25 lignes x 80 caractères ! On se demandait même ce qu'on pourrait faire d'autant ! S'en est suivie la décentralisation du traitement des prêts personnels ; en effet, à la base, les prêts étaient enregistrés sur des bordereaux puis saisis au siège de la banque. Décentraliser cette saisie en agence a été un véritable progrès. A la fin des années 1980, la Banque a fait l'opération « Mille Postes », il s'agissait de fournir un poste informatique à chaque collaborateur. Les années 1990 ont suivi avec l'apparition de la micro-informatique et l'évolution des réseaux. Les premiers logiciels bancaires tournaient sous DOS, il a fallu attendre fin 2000 pour découvrir le nouveau logiciel Symphonie tournant sous Windows, c'est cette plateforme qui est encore utilisée aujourd'hui. La fusion de la Banque Populaire de Lorraine et de la Banque Populaire de Champagne en 2002 a encore été un tournant dans l'histoire informatique de la Banque puisqu'elle a engendré un grand déploiement de réseaux. L'informatique de la Banque Populaire de Lorraine (Lorraine-Champagne par la suite) trouve son identité dans sa construction au fil des évolutions ; chaque étape de sa croissance s'est basée sur la précédente, sans jamais repartir de zéro. Elle a toujours été parmi les précurseurs dans l'utilisation et le déploiement de nouvelles technologies (comme pour le premier automate de banque qui a été implanté à Thionville). Actuellement, l'informatique de la BPLC reste une entité indépendante à l'affût des nouvelles technologies (Minitel, Internet, SMS, I-Mode…).

A l'exception de la Banque Populaire de Champagne, les autres Banques Populaires se sont retirées du Centre Informatique.

Le CIM est dirigé par M. Tournebize, directeur de l'Informatique, et a actuellement un effectif de 103 salariés répartis comme suit : 3 personnes à la direction, 48 personnes dans le département Etudes et Développement Bancaire et 52 personnes dans le département Systèmes et Réseaux. 22 de ces employés sont salariés d'entreprises extérieures, prestataires de services.

Voici son organigramme :

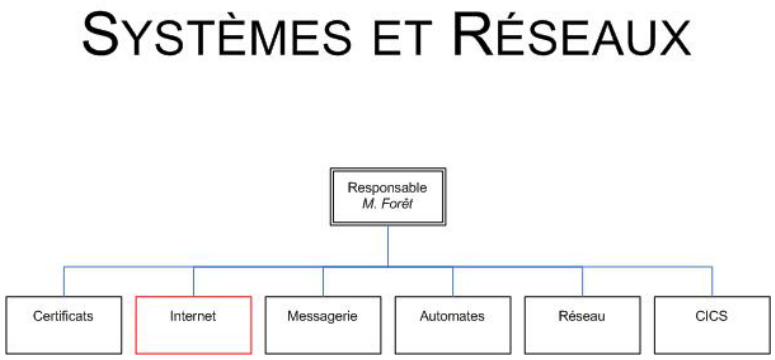


Le CIM est un service informatique indépendant, qui veille à la continuité du service informatique tant au niveau interne à la banque qu'au niveau client. Son domaine d'action va des applications bancaires à la messagerie interne, en passant par le réseau informatique à proprement parler. Son activité consiste également en une veille technologique, afin de mettre en œuvre des équipements de plus en plus performants et modernes.

Les deux départements dont est composé le CIM, Etudes et Systèmes, sont eux-mêmes divisés en services, où chaque collaborateur joue un rôle à part entière. Chaque service développe son domaine, mais travaille également en collaboration étroite avec ses pairs, tant que faire se peut, afin que chaque objectif soit atteint de manière optimale et que toutes les opérations soient compatibles.

Mon stage s'est déroulé au sein du service Systèmes et Réseaux du Département Systèmes et Réseaux, dirigé par Robert Forêt. Il compte 10 personnes au total dont 3 personnes travaillant pour une société de service extérieure. Ce service s'occupe du réseau (architecture, maintenance, choix des matériels, mise en oeuvre), d'Internet, de la messagerie, des certificats, des automates et de la partie application système du système central.

Voici la structure du service :



L'équipe *Certificats* s'occupe de l'authentification des postes de travail se connectant à une application en Nomade ou à des postes clients pour des échanges. En effet, chaque poste se connectant, doit être identifié et reconnu grâce à son certificat. Actuellement, toutes les applications bancaires sont en train de migrer vers l'intégration maximale du cryptage en utilisant les certifications.

L'équipe *Internet* englobe tout ce qui concerne les relations avec le Web : gestion des serveurs de services Internet, firewall, hébergement, accès au réseau, messagerie externe. C'est au sein de cette équipe que j'ai effectué mon stage.

L'équipe *Messagerie* travaille sur la messagerie interne à la banque, basée sur le logiciel Lotus Notes. Ce logiciel, n'est pas qu'un logiciel de messagerie, mais englobe toutes les connaissances de la banque sous forme de bases documentaires. C'est un pilier du travail quotidien de chaque collaborateur de la banque.

L'équipe *Automates* s'occupe principalement des Guichets Automatiques de Banque (appelés GAB), de la mise en œuvre des logiciels système de ces machines, de leur mise en place sur le réseau, de la cryptographie associée, des applications et de la maintenance.

L'équipe *Réseau* travaille sur l'architecture, la mise en œuvre et l'optimisation du réseau.

Enfin, l'équipe *CICS* concerne le serveur Host (machine qui supporte toutes les données et applications bancaires, c'est le cœur de la banque).

Présentation du stage

A l'heure ou j'ai posé ma candidature pour un stage à la Banque Populaire Lorraine-Champagne, l'informatique venait d'entrer dans une ère de refonte complète de son réseau de communications. Ce réseau étant en perpétuelle évolution, il s'agit là d'une refonte plus importante, avec pour objectif une optimisation du site central ainsi que la mise en œuvre d'un nouveau réseau voix/data offrant des possibilités variées.

En janvier 2005, le processus était lancé. Dans ce contexte, M. Forêt, directeur-adjoint des Systèmes et Réseaux, était ouvert à toutes propositions et idées nouvelles afin d'éventuellement améliorer le projet. C'est dans ces conditions que l'arrivée d'un(e) stagiaire l'a enthousiasmé. La mission qui m'a été confiée dans le cadre de mon stage a été la **mise en place d'un back-up du site Internet**. Cela fait partie du projet de fiabilisation de l'accès Internet de la banque. Outre ce projet, je devais également étudier des **propositions envisageables pour la nouvelle architecture du réseau**.

Mon stage débutant début Avril 2005, j'ai été conviée à plusieurs réunions courant Février et Mars 2005 afin de commencer mon stage en étant familiarisée avec les bases du projet. J'ai trouvé cette initiative très intéressante et valorisante : ces réunions m'ont permis d'approcher l'infrastructure et de faire connaissance avec l'équipe travaillant sur ce projet. Bien entendu, avant de débuter le projet la banque avait fait un appel d'offres. Différents opérateurs avaient répondu présents. Au final, France Télécom/Transpac est sorti du lot, dans le cadre de relations commerciales durables et de propositions techniques attrayantes.

8 Février 2005 : première réunion d'une demi journée avec un ingénieur commercial de chez France Télécom/Transpac, les membres de l'équipe Internet, ainsi que des développeurs du service des études. Il s'agissait là d'étudier les différentes architectures possibles à mettre en œuvre à partir de l'architecture actuelle, et de définir les besoins.

22 Mars 2005 : seconde réunion d'une journée au siège de la BPLC avec l'équipe de France Télécom/Transpac/Equant ainsi que toute l'équipe des responsables du Centre Informatique de Metz. Le but était d'étudier le passage au nouveau réseau voix/data (NRVD) dont la mise en place « expérimentale » avait déjà commencé sur 3 agences bancaires. Ont été évoqués, les problèmes rencontrés, la planification et la fiabilisation de l'accès internet.

Nous aborderons ces domaines dans la suite de ce rapport.

Découverte de l'infrastructure

L'arrivée dans un nouveau contexte technique et complexe n'est pas mince affaire. Il s'agissait pour moi d'intégrer au plus vite le fonctionnement de l'informatique à la BPLC. Dès le premier jour, on a pris le temps de me faire visiter les infrastructures et de m'expliquer tout le réseau. Dans ce chapitre, je vais vous présenter les équipements informatiques puis le plan du réseau.

1- Les moyens du Centre Informatique de Metz

Le Centre Informatique de Metz se divise en deux sites centraux :

- un site de production à Metz-Nord (zone des Deux-Fontaines),
- un site de back-up à Metz-Centre (quartier Gare).

Chaque site possède un ordinateur central de respectivement 192 MIPS et 220 MIPS pour assurer le traitement informatique de la BPLC. Ces ordinateurs sont :

Metz-Nord (production) :

- 1 ordinateur IBM Z800/2066-001
  * refroidi par air
  * 32 canaux ESCON (dont 4 canaux émulés en canaux parallèles par des boîtiers 9034)
  * 7 boîtiers 9034 - Emulation de canaux ESCON en canaux parallèles
  * 1 carte OSA Express Fast Ethernet FC 2366
  * 8 gigaoctets de mémoire centrale
  * 192 mips (1 moteur de 192 mips)

- système d'exploitation IBM Z/OS 1.4

- 4 moniteurs TP IBM CICS V4 actifs

- 2 moniteurs TP IBM CICS V4 back-up CB

- 2 moniteurs TP IBM CICS V4 de tests

- 1 V2X Storagetek avec 1890 gigaoctets de disque

- 1 VSM4 Storagetek avec 1250 gigaoctets de disque

- 1 librairie Timberwolf 9740 Storagetek de 326 slots avec 2 lecteurs 9840

- 1 lecteur Timberline 9490 Storagetek

- 1 routeur CISCO 7204 et 2 routeurs CISCO 7206

- 1 imprimante IBM 3900 0W1, 235 pages/minute théorique

- 1 imprimante Fujitsu 3056M, 217 pages/minute théorique

- matériel de façonnage-mise sous pli extraits Kern, 18.000 enveloppes/heure (si 1 pli par enveloppe)

- matériel de façonnage-mise sous pli lettres Böwe, Pitney Böwes

Metz-Centre (machine de back-up, dormante) :

- 1 ordinateur IBM CMOS 9672 modèle R26
  * refroidi par air
  * 12 canaux parallèles
  * 36 canaux ESCON
  * 2 cartes OSA2 ENTR (Ethernet/Tocken ring)
  * 2 gigaoctets de mémoire centrale
  * 220 mips (2 moteurs de 110 mips)

- système d'exploitation IBM Z/OS 1.4

- 1 V2X Storagetek avec 1890 gigaoctets de disque

- 1 VSM Storagetek avec 460 gigaoctets de disque

- 1 librairie Timberwolf 9740 Storagetek de 326 slots avec 2 lecteurs 9840

- 1 lecteur Timberline 9490 Storagetek

- 1 routeur CISCO 7204 et 1 routeur CISCO 7206

Les ordinateurs sont dédiés à la gestion des CICS (Customer Information Control System). Un CICS est un moniteur de traitement de l'information OnLine. Nous n'entrerons pas dans les détails puisque cela n'était pas l'objet de mon stage.

Logiciels site central :

- systèmes d'exploitation : IBM Z/OS 1.4

- protocoles de communication : VTAM, TCP/IP

- moniteurs télétraitement : IBM CICS.V4

- système de gestion de bases de données CA DATACOM

- langages de développement : IBM OS/COBOL et IBM COBOL for OS
  (+ un peu de CA IDEAL, un résiduel de Assembleur et quelques IBM PL/1)

- gestionnaire de sources : CA Librarian

Réseaux :

- protocoles de communication :
  * TCP/IP : TN3270, NOTES ,ORACLE, SYMPHONIE, Bornes MILS et Internet, GABS
  * IPX pour l'administration NETWARE
  * SNA pour la communication inter BP
  * XOT pour les ETEBAC, MINITEL et RCB

- connexion réseau Groupe des BP

- réseaux locaux en Ethernet (restent un token ring à Metz-Nord et un à Metz-Centre)

- 1500 postes de travail

- 180 serveurs Novell NETWARE

- 135 routeurs agence

- 25 routeurs GABS remote

- 4 serveurs Lotus NOTES (Systeme d'Exploitation NT4)

- 4 serveurs ORACLE

- 6 serveurs dédiés (Crédence, IT2, BAFI)

- 273 GAB (Guichet Automatique Bancaire)

- 81 MILS (Imprimante Libre Service)

Logiciels sur micro-ordinateur :

- systèmes d'exploitation : Windows 98 (1000), Windows 2000 (5), Windows XP (500)

- langage de développement :
  PC Soft Windev pour le développement poste de l'exploitant
  PC Soft Webdev et Microsoft ASP et VB pour le développement Internet

- navigateurs Internet Explorer (5.5 ou 6), Netscape Communicator (4.6)

- Anti virus SOPHOS

- Open Office en général, Office 2000 dans certains cas

- Acrobat Reader 5.0

- suite bureautique Lotus SmartSuite (123, Notes 4.6, Amipro, Word Pro)

Internet

- Fournisseur d'accès : utilisation du service de collecte FREESP de Transpac (RTC/Numéris avec évasion Internet)
  * Authentification sur deux serveurs RADIUS
  * Maintien de l'accès par le Max4000

- Hébergement Serveurs Internet :
* Infrastructure :
    - 2 routeurs CISCO 3620 secourus en HSRP
    - 1Firewall NG de Checkpoint (5 interfaces réseaux)

    - 1 Antivirus analysant le flux SMTP et FTP
        * version de production ESPG 3.5
        * version de production ESPG 4 avec fonctionnalités anti-spam
    - 1console de management FW
    - 2 serveurs de noms de domaine (DNS)
    - 1 serveur de messagerie (+ 1 serveur de rebond de messages)
    - 1 passerelle NOTES/INTERNET

* Serveurs Clients :
    - 8 serveurs clients devant le FW
    - 15 serveurs clients protégés par le FW
    - 3 serveurs d'hébergements mutualisés
    - 1 serveur de statistiques WEBTRENDS

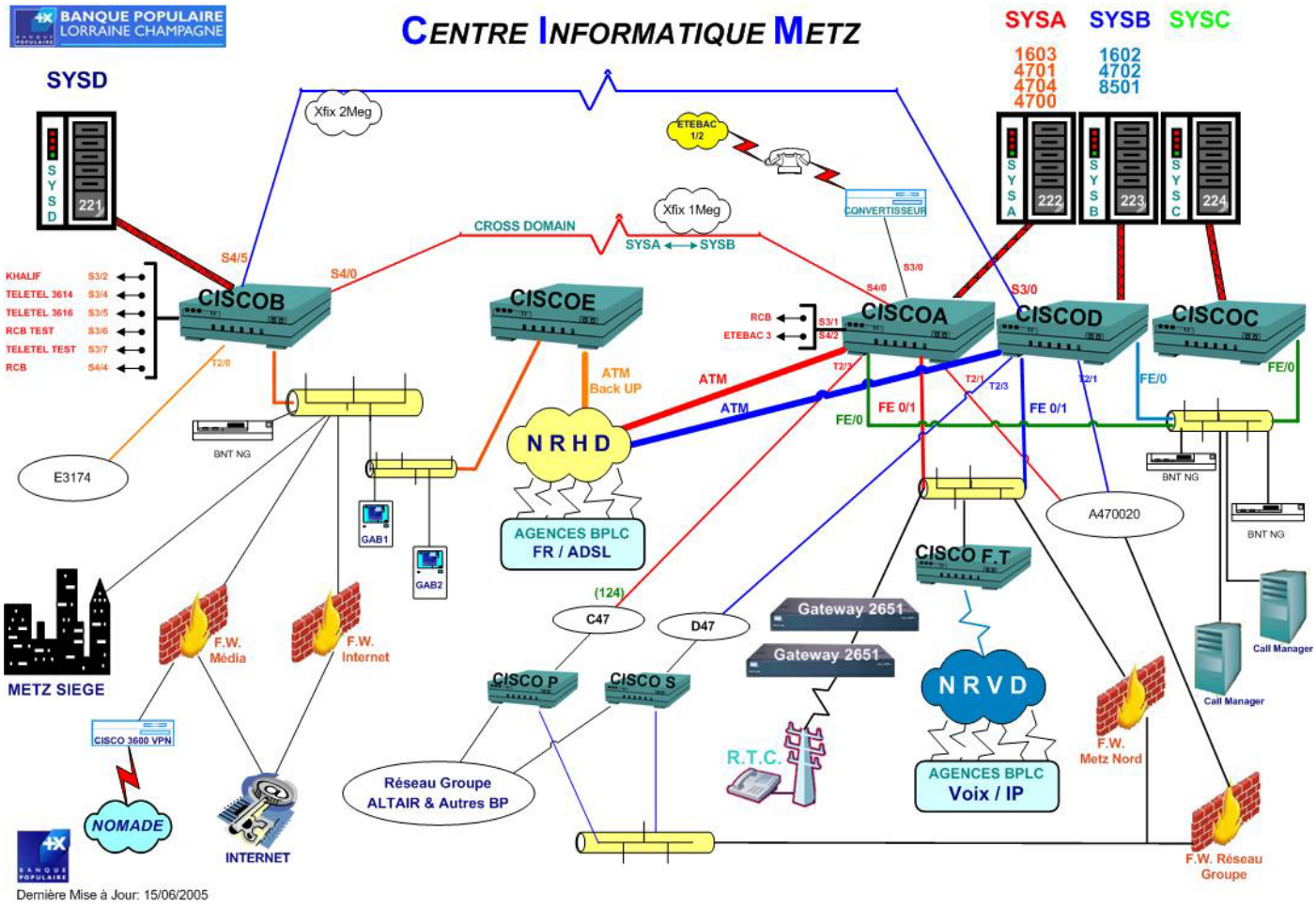
* Serveurs Banque :
    - 3 serveurs pour le site Internet (Vitrine, Compte clients et Compte employés)
    - 1 serveur d'e-commerce
    - 1 serveur d'envoi de SMS (Moviplus)
    - 1 serveur d'envoi de SMS (SMS+)
    - 1 serveur de certificats
    - 1 serveur Intranet (e-dimensions, e-offensive et patrithèque)

* Sécurité :
    - 1 FW Groupe (Metz Nord)
    - 1 FW Média (Metz Centre)

* Nomade :
    - 1 CISCO 3660 (N° d'appel gratuit)
    - 1 accès via INTERNET par le FW Média
    - 1 serveur RADIUS d'authentification et de connexion VPN

2- Le réseau

Voici le schéma du réseau actuel (c'est-à-dire avant refonte) :



Les adresses IP ont été retirées dans un souci de confidentialité. Vous pourrez trouver en annexe I ce schéma en grand format.

Différents types de liaisons sont utilisés pour connecter entre elles les différentes parties du réseau. Ils sont indiqués sur le schéma ci-dessus (ATM, ligne Transfix 1M/2M, liaisons canal, série, Ethernet…).

Sur ce schéma, on peut distinguer les parties Internet, NRHD et NRVD. Nous aborderons ces points plus en détail par la suite.

Missions

Comme je vous l'ai présentée, la mission principale qui m'a été attribuée pendant mon stage concerne la fiabilisation de l'accès Internet ainsi que l'optimisation du site central. Cependant, M. Forêt m'a permis ponctuellement de découvrir d'autres domaines de l'informatique de la Banque Populaire Lorraine-Champagne comme les automates, la gestion réseau et les services mails. Je vais ici vous présenter ces différentes expériences ludiques et enrichissantes en commençant par les plus brèves ; nous terminerons par les plus importantes.

1- La Gestion Réseaux

Une grande structure comme la BPLC, avec plus de 1 400 salariés et 1 500 postes informatiques, rencontre évidemment des aléas quotidiens sur l'ensemble de ses équipements. Dirigée par M. Daumal, la Gestion Réseaux regroupe une équipe de techniciens chargés du bon fonctionnement du parc informatique et une équipe hotline qui prend en compte les appels, résout les incidents mineurs et oriente les autres.. Ils sont responsables de l'attribution et de la maintenance des postes et de tout le matériel informatique de la banque, qui est répertorié grâce à des codes-barres. Ils s'occupent également du déploiement de logiciels et applications chez les utilisateurs.

J'ai eu l'occasion de passer une demi-journée au SVP, c'est la plateforme qui gère tous les incidents qui ont lieu sur le réseau : ils couvrent tous les domaines allant de l'impression aux automates en passant par le réseau à proprement parler. Cinq personnes composent l'équipe dirigée par M. Lelot, trois d'entre elles s'occupent principalement de l'accueil téléphonique et de la répartition des incidents.

Le SVP occupe une grande pièce depuis laquelle l'équipe a la possibilité de surveiller tout ce qui se passe sur le réseau, grâce à l'outil « What's up » ainsi que des postes de surveillance, pour le Minitel ou les automates par exemple. Les agences (et le siège) ont un numéro de téléphone unique à composer pour joindre la Gestion Réseaux et leur relater les problèmes rencontrés. Une fois l'appel reçu, l'opérateur téléphonique peut aider la personne à le régler immédiatement ou alors faire une fiche d'incident pour qu'il soit traité par une personne compétente au plus vite.

Les opérateurs traitent en moyenne 80 appels par jour. Entre 1/4 et 1/3 des appels sont inutiles et concernent une imprimante bloquée ou un poste à redémarrer. Ils reçoivent aussi des appels leur signalant l'indisponibilité d'un automate, dans ce cas, ils ont la possibilité de vérifier à distance l'état de celui-ci et d'identifier le problème (problème de billets ou panne), ils peuvent également le fermer ou le mettre en fonctionnement dégradé. En cas de panne

d'un automate, un fax est envoyé immédiatement à la société de maintenance pour une intervention au plus vite.

D'autres appels concernent des opérations d'installation ou des problèmes connus. Dans ce cas, une base Notes a été créée : chaque technicien a créé des tutoriels traitant des problèmes courants qu'un néophyte peut régler en autonomie. Tout le matériel est également recensé avec photographies et notices techniques afin de permettre aux techniciens de visualiser ce le matériel en même temps que son interlocuteur. J'ai eu l'occasion de consulter cette base de données, je trouve que c'est une véritable mine d'or qui a du nécessiter des heures de travail. C'est une initiative à retenir ! Certains collaborateurs désirent parfois utiliser un logiciel qui n'est pas installé sur leur poste, ou même un nouveau poste. Dans ce cas, ils doivent remplir un formulaire de « demande de travaux » et une solution est trouvée le plus rapidement possible.

A côté du SVP, les techniciens de la Gestion Réseaux réparent des appareils défectueux tant au niveau matériel qu'au niveau logiciel. Ils disposent d'un atelier, où sont également entreposés des anciennes machines dont on peut récupérer les composants. C'est par là que transitent tous les équipements.

De cette expérience d'observation, je retiendrai une organisation sans faille qui permet d'être le plus efficace possible face aux incidents. Cela m'a permis de découvrir les structures mises en places dans les grandes entreprises et que je n'imaginais pas.

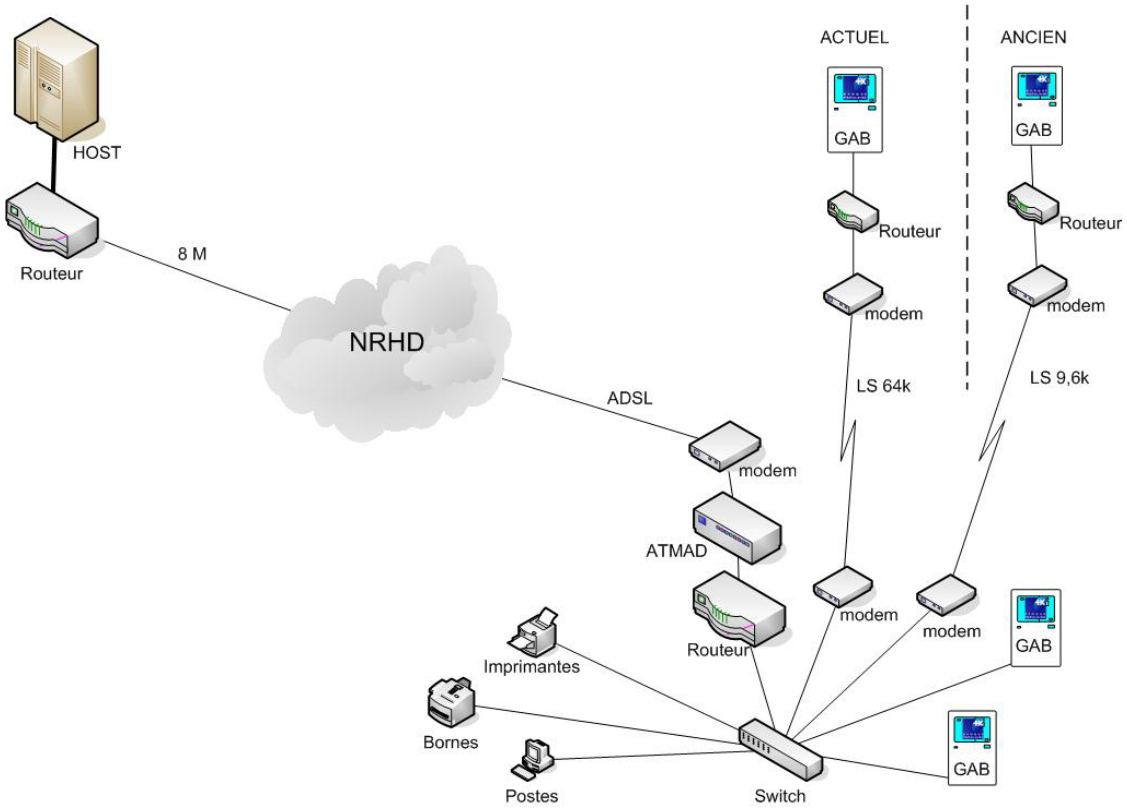
2- Automates

Les automates sont les Guichets Automatiques de Banque, ceux que l'on a l'occasion de voir fleurir dans nos rues à l'heure actuelle. J'ai eu l'occasion de passer plusieurs demi-journées avec les personnes qui s'en occupent : Mme Mercy du département Système et Réseaux et M. Bertrand de la Gestion Réseaux, technicien de maintenance.

Les G.A.B. sont de simples ordinateurs à l'intérieur d'une armoire en métal : ils sont composés d'une tour, d'un écran de contrôle et il y a possibilité d'y brancher clavier et souris (les plus récents ont même un écran TFT, un clavier et un pavé tactile intégré). La partie « billets » se trouve en dessous, dans un coffre-fort. Ils sont reliés au réseau informatique en IP (à l'heure actuelle encore beaucoup de banques ont leurs G.A.B. en X25, la Banque Populaire a fait partie des premières à passer ses G.A.B. de SDLC en IP). A l'intérieur de l'armoire, il y a un lecteur de carte, une imprimante pour le ticket ; les billets sont introduits dans le distributeur à l'intérieur de cassettes. Un G.A.B. peut en contenir quatre, il y a également une cassette de rebus pour récupérer les billets abîmés. Les anciens G.A.B. en SDLC fonctionnaient sous OS-2, les plus récents fonctionnent sous Windows (2000, et maintenant XP). Ces systèmes d'exploitation sont tout de même allégés afin de ne pas être encombrés par des fonctionnalités inutiles. Un aspect important des G.A.B. est la structure en couches logiques. Les G.A.B. de la BPLC sont de la marque Diebold.

Les G.A.B. sont déployés sur un réseau isolé, et les données qu'ils échangent sont cryptées. Actuellement, un firewall est en train d'être testé pour assurer une meilleure sécurité du réseau des G.A.B. Chaque G.A.B. dépend d'une agence et est à l'intérieur d'elle ; certaines agences ont des G.A.B. éloignés comme par exemple l'agence de Rombas et le guichet de Walibi Lorraine ; dans ce cas, le G.A.B. est relié au réseau de l'agence par une liaison spécialisée à 64k.

Voici le schéma de raccordement des G.A.B :



Par la suite, j'ai eu l'occasion de partir en intervention avec M. Bertrand. Nous nous sommes rendus à l'agence bancaire de Rombas puis à l'automate du parc Walibi Lorraine afin de remettre le G.A.B. en service à l'occasion de la réouverture annuelle du parc. Deux nouveautés : l'ancienne ligne spécialisée à 9,6k entre l'agence et le parc avait été remplacée par une ligne à 64k et le remplacement de l'ancienne machine par une neuve. Nous avons d'abord été vérifier en agence que les bons raccordements avaient été faits entre le routeur de l'agence et le modem France Télécom. Ensuite nous nous sommes rendu sur l'emplacement du G.A.B. afin d'y installer un routeur (CISCO 805). C'est une installation très rapide : il suffit de raccorder le routeur au réseau et au G.A.B, de lui attribuer une adresse IP et de vérifier par téléphone avec une personne restée au siège si tout fonctionne correctement. Le lendemain, le nouveau guichet était implanté.

En deuxième lieu, je suis repartie avec M. Bertrand pour faire une mise à jour de système d'exploitation sur un G.A.B. à la Foire Internationale de Metz. C'est un G.A.B. particulier qui n'ouvre que lors des manifestations à la Foire, de plus, la configuration des cassettes de billets qu'il contient est exceptionnelle. Tout ce qui touche à l'argent est naturellement très surveillé, l'applicatif Diebold de gestion de l'automate est donc préréglé pour une configuration classique. Lors de la mise à jour, nous avons du porter une attention particulière à la configuration des cassettes de billets. Si l'applicatif détecte une erreur de

correspondance entre la cassette de billets qui a été insérée (les cassettes sont reconnues grâce à des plots) et la cassette qui a été programmée, l'appareil se bloque.

Cette intervention a nécessité la présence d'une personne de l'entreprise qui s'occupe des G.A.B. pour la sécurité. En effet, cette personne est habilitée à ouvrir local technique ainsi que l'automate, elle doit rester à nos côtés pendant toute la durée de l'opération. L'installation de la nouvelle version s'est déroulée sans problème et a duré un peu plus de trois heures. A la fin de celle-ci, il faut transmettre les clefs cryptographiques à la personne qui s'occupe des G.A.B. au siège pour qu'elle vérifie si il fonctionne bien ; cet automate étant éloigné par rapport à une agence, nous ne disposions pas de connexion internet pour envoyer le fichier. Nous avons du récupérer les fichiers sur disquette et faire un aller-retour en auto. Une fois l'installation terminée, le guichet a été laissé en service pour le public.

A mon retour, j'ai rédigé un mini mode d'emploi pour faciliter les interventions futures sur ce GAB particulier.

3- Messagerie

A l'heure actuelle, le principal moyen de communication écrite des entreprises avec l'extérieur est devenu la messagerie électronique. C'est également un support commercial considérable. La BPLC dispose d'un serveur de messagerie (POP/SMTP) pour sa messagerie ainsi que celles de ses clients Internet. J'ai passé quelques demi-journées avec M. Wagner qui s'occupe de « Messa », c'est ainsi qu'est nommé ce serveur. J'ai ainsi pu en voir le fonctionnement et être confrontée aux problèmes quotidiens liés aux « mails ».

Tout d'abord, quelques explications techniques :

Le courrier électronique est considéré comme étant le service le plus utilisé sur Internet. Ainsi la suite de protocoles TCP/IP offre une panoplie de protocoles permettant de gérer facilement le routage du courrier sur le réseau.

Le **protocole SMTP** (*Simple Mail Transfer Protocol*) est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole SMTP fonctionne grâce à des commandes textuelles envoyées au serveur SMTP (par défaut sur le port 25). Chacune des commandes envoyées par le client (validée par la chaîne de caractères ASCII *CR/LF*, équivalent à un appui sur la touche entrée) est suivi d'une réponse du serveur SMTP composée d'un numéro et d'un message descriptif.

Voici un scénario de demande d'envoi de mail à un serveur SMTP :

- Lors de l'ouverture de la session SMTP, la première commande à envoyer est la commande *HELO* suivie d'un espace (noté <*SP*>) et du nom de domaine de votre machine (afin de dire "bonjour je suis telle machine"), puis valider par entrée (noté <*CRLF*>). Depuis avril 2001, les spécifications du protocole SMTP imposent que la commande HELO soit remplacée par la commande *EHLO*.
- La seconde commande est "*MAIL FROM:*" suivie de l'adresse email de l'expéditeur. Si la commande est acceptée le serveur renvoie le message "*250 OK*"
- La commande suivante est "*RCPT TO:*" suivie de l'adresse email du destinataire. Si la commande est acceptée le serveur renvoie le message "*250 OK*"
- La commande *DATA* est la troisième étape de l'envoi. Elle annonce le début du corps du message. Si la commande est acceptée le serveur renvoie un message intermédiaire numéroté *354* indiquant que l'envoi du corps du mail peut commencer et considère l'ensemble des lignes suivantes jusqu'à la fin du message repéré par une ligne contenant uniquement un point. Le corps du mail contient éventuellement certains des en-têtes suivants :
  - Date
  - Subject
  - Cc
  - Bcc
  - From

  Si la commande est acceptée le serveur renvoie le message "*250 OK*"

Le **protocole POP** (*Post Office Protocol*) permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion. Il existe deux principales versions de ce protocole, POP2 et POP3, auxquels sont affectés respectivement les ports 109 et 110 et fonctionnant à l'aide de commandes textuelles radicalement différentes. Tout comme dans le cas du protocole SMTP, le protocole POP (POP2 et POP3) fonctionne grâce à des commandes textuelles envoyées au serveur POP. Chacune des commandes envoyées par le client (validée par la séquence *CR/LF*) est composée d'un mot-clé, éventuellement accompagné d'un ou plusieurs arguments et est suivie d'une réponse du serveur POP composée d'un numéro et d'un message descriptif.
Le protocole POP3 gère l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe, il n'est par contre pas sécurisé car les mots de passe, au même titre que les mails, circulent en clair (de manière non chiffrée) sur le réseau. En réalité, il est possible de chiffrer le mot de passe en utilisant un algorithme et ainsi bénéficier d'une authentification sécurisée. Toutefois, cette commande étant optionnelle, peu de serveurs l'implémentent. D'autre part le protocole POP3 bloque la boîte aux lettres lors de la consultation, ce qui signifie qu'une consultation simultanée par deux utilisateurs d'une même boîte aux lettres est impossible.

Fonctionnement de la messagerie :

Les mails entrants arrivent sur le firewall Internet qui fait office de proxy (intermédiaire entre le réseau local et Internet). Sur celui-ci, une règle est programmée pour envoyer les mails entrants sur l'antivirus/antispam. Une fois que le mail est validé par le firewall, il est renvoyé vers le serveur de messagerie.

Un mail sortant part du serveur de messagerie Messa, va au firewall qui le fait retourner sur le concierge et repart vers le firewall pour finalement sortir.

A la BPLC, il y a deux MX. MX fait référence à une particularité du DNS concernant les mails, le MX d'un domaine correspondant au serveur sur lequel seront envoyés les e-mails. On trouve sur un domaine différents types de champs qui peuvent servir à y accéder. Le MX est un champ constitué d'un chiffre et d'un nom d'hôte (pas d'adresse IP) qui permet de définir avec une priorité le serveur qui recevra les e-mails envoyés sur ce domaine (0 étant la priorité la plus élevée). Lorsqu'un utilisateur envoie un courrier électronique à une adresse (utilisateur@domaine), le serveur de courrier sortant interroge le serveur de nom ayant autorité sur le domaine afin d'obtenir l'enregistrement MX. Il peut exister plusieurs MX par domaine, afin de fournir une redondance en cas de panne du serveur de messagerie principal.

A chaque fois que j'ai été en observation avec M. Wagner, c'est qu'il y avait un problème sur le serveur Messa. En effet, ce serveur est régulièrement saturé, c'est-à-dire qu'il n'arrive pas à transmettre assez rapidement tous les messages qui lui sont envoyés, son spool est donc rempli. En temps normal, il y a une vingtaine voire une centaine de messages dans le spool, mais lors d'une saturation, ce nombre dépasse les 1000 et peut monter jusqu'à plus de 20 000. Les techniciens disposent d'une application dans laquelle ils entrent un quota qui leur permet d'en être avertis par SMS sur leur téléphone mobile de tout débordement du serveur.

Ces problèmes de débordements sont relativement récents et correspondent à la montée en nombre des spams. C'est un problème que j'avais abordé oralement avec M. Monteiro durant cette année scolaire. Comment ce problème se traduit-il au niveau de Messa ? C'est très simple : les expéditeurs de spam envoient leurs « pourriels » à des adresses générées au hasard (bien souvent des noms anglais très répandus ou récupérés sur Internet) en les associant à des noms de domaines. De plus l'adresse mail donnée en en-tête est une adresse inexistante. C'est un envoi massif et simultané de ces mails qui sature le serveur en réception. S'en suit un message d'erreur généré automatiquement par Messa pour signifier à l'expéditeur que le destinataire n'existe pas. Mais, puisque l'adresse du spammeur est fictive, le serveur d'en face va renvoyer un message d'erreur lui aussi. Nous entrons donc dans un processus sans fin qui génère beaucoup de problème.

Plus de 80%du trafic est du aux spams. Lors d'encombrements, on peut attendre que les attaques de spams se tassent, mais il est aussi utile de faire un peu de ménage manuellement dans le spool, en repérant par exemple, des messages de taille identique. C'est une tâche quasi-irréalisable et de plus, c'est toujours une opération délicate car il s'agit de ne surtout pas supprimer un message réellement destiné à un collaborateur.

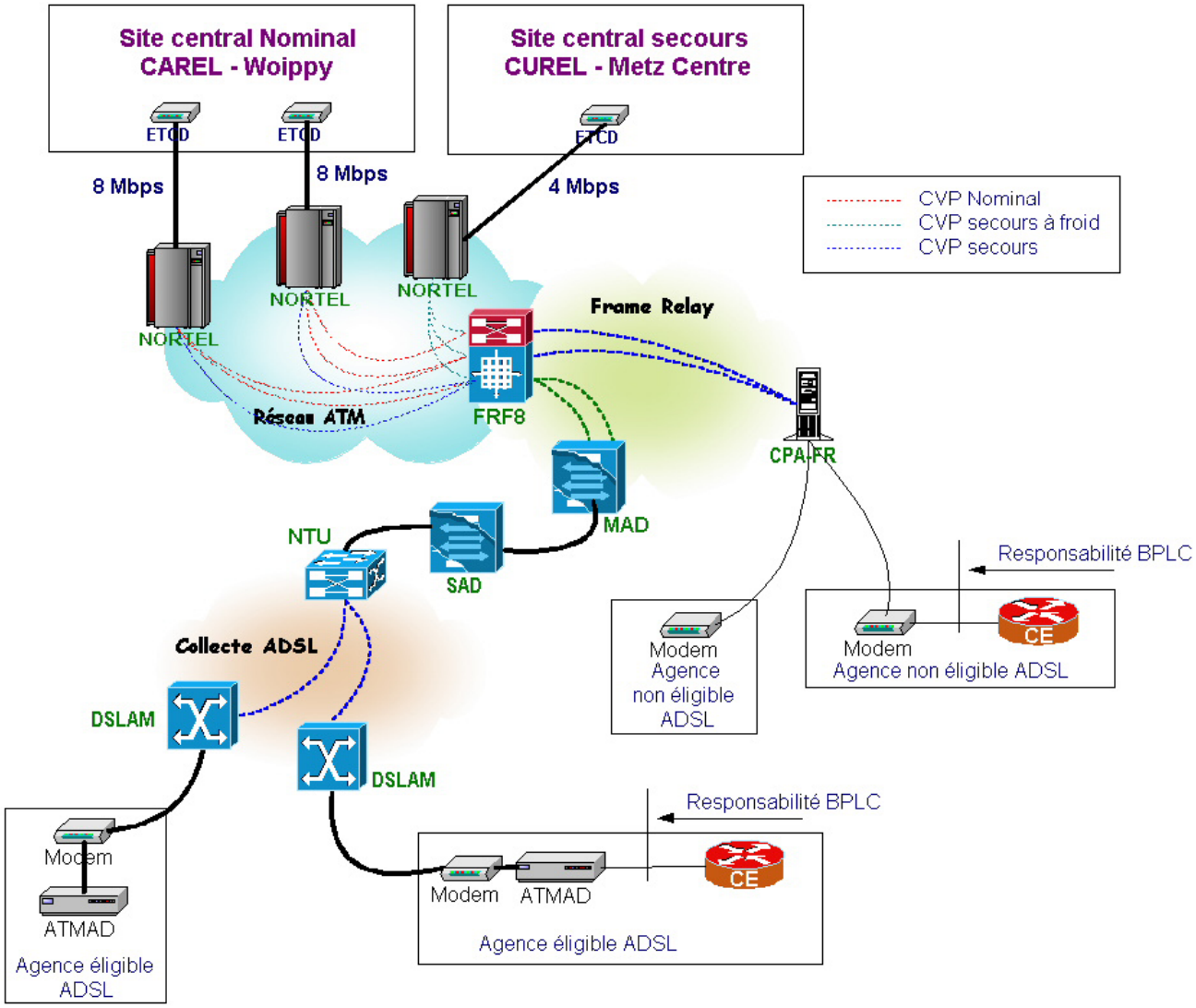
Notre projet, (pas encore réalisé à cette date) est d'écrire un script agissant sur les messages entrants dans ISMTPOnArrival afin de le supprimer ou de le rediriger vers une boîte poubelle. Pour l'instant nous avons mis entre parenthèses nos recherches sur ce sujet afin de nous consacrer à la partie Internet.

4- Optimisation du site central

Comme je l'ai présenté, le Centre Informatique de la BPLC est entré dans une période de refonte de son réseau. Dans le cadre de cette avancée, il est nécessaire de distinguer l'optimisation du site central NRHD (« ancien » Nouveau Réseau Haut Débit) et la mise en œuvre du NRVD (Nouveau Réseau Voix Data).

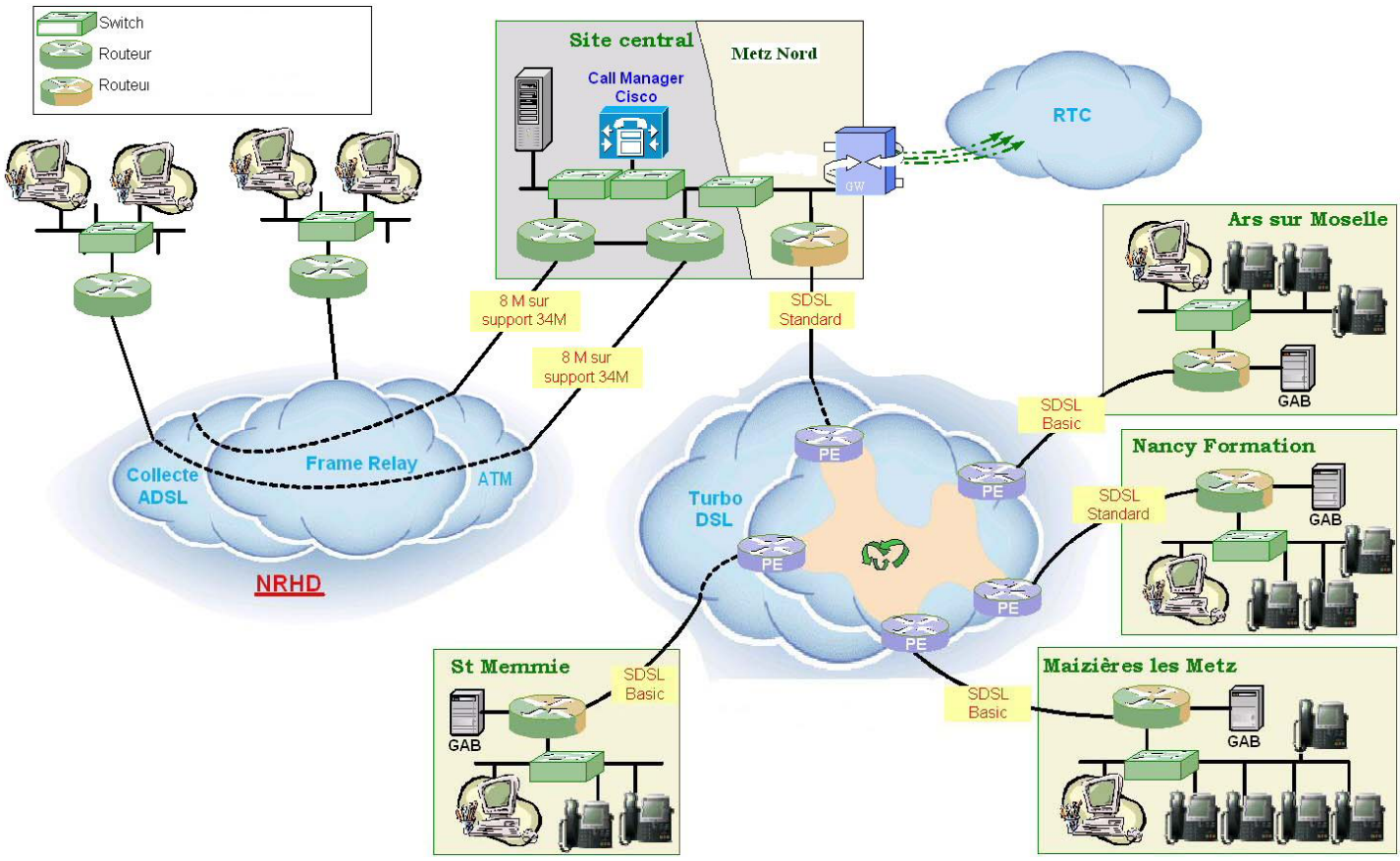
En quoi cela consiste-t-il ?

Le réseau NRHD est un réseau haut-débit qui a été mis en place il y a deux ans afin de relier les agences bancaires au réseau. L'infrastructure est fournie par France Télécom/Transpac/Equant. En voici in schéma :



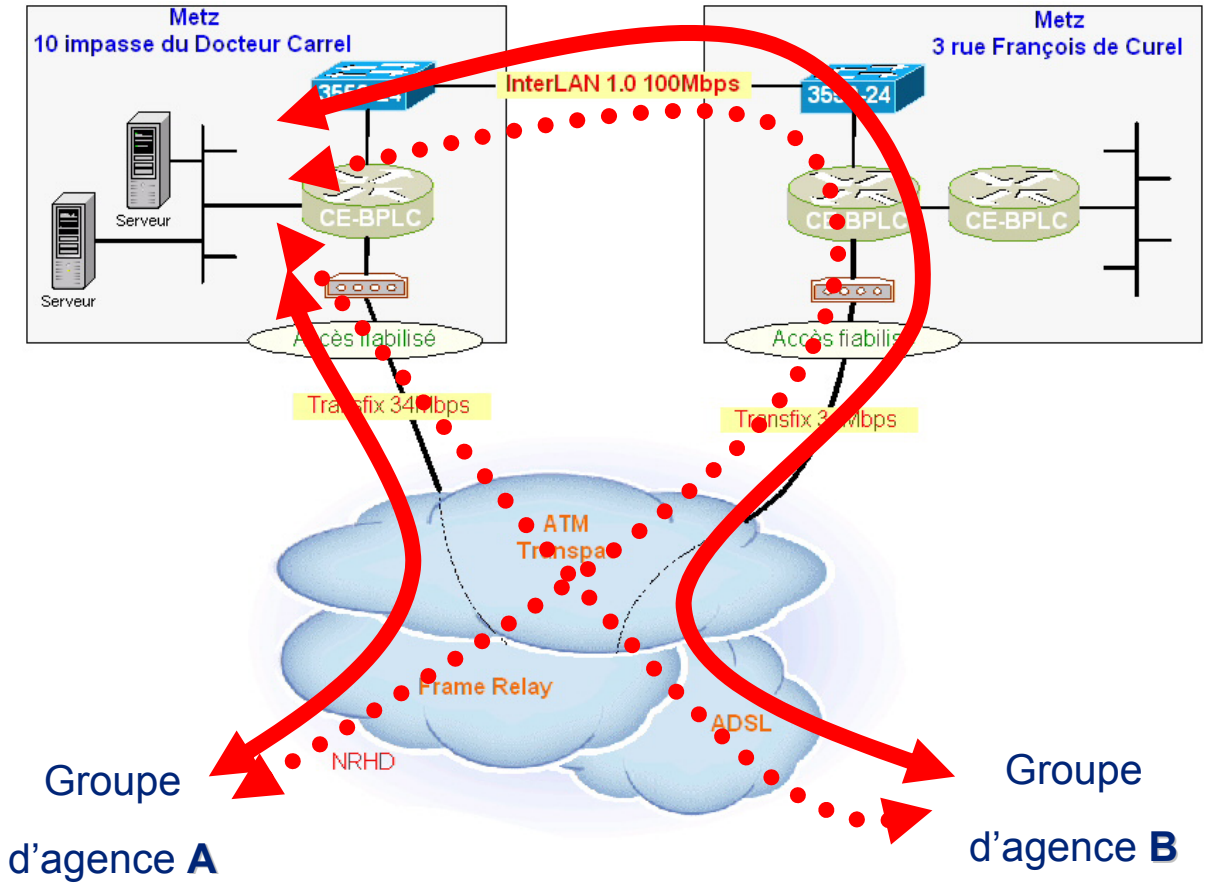
Comme on peut le voir sur ce schéma ainsi que sur celui que vous trouverez en annexe I, le NRHD est relié en ATM aux routeurs Cisco 7206 et 7204 de Metz-Nord et Metz-Centre. Les agences ont ainsi accès aux informations bancaires stockées sur le host et à Internet. Le reste de la liaison est supporté par le réseau France Télécom. La majorité des agences est reliée en ADSL (96k en débit descendant, 48k en débit montant), mais il existe encore à l'heure actuelle des problèmes d'éligibilité pour les lignes ADSL : les agences non éligibles sont reliées en frame relay. Le frame relay est un mode de transfert de données basé sur la commutation par paquets permettant de transmettre, à haut débit et sur de grandes distances, des quantités importantes de données.

Le réseau NRVD est un réseau haut-débit qui est actuellement en plein déploiement. Il s'agit de relier au réseau toutes les agences avec une liaison de type SDSL afin de remplacer la téléphonie classique par de la téléphonie IP. Pour l'instant, le NRVD cohabite avec le NRHD, mais le but est bien que le NRHD soit remplacé par le NRVD. A l'heure actuelle, seules six agences sont reliées (Saint Memmie, Maizières-lès-Metz, Ars-sur-Moselle, Semart, Golbey, Nogent-sur-Seine), elles servent de pilotes afin d'éventuellement améliorer la qualité du réseau. Voici un schéma précisant la mise en place structurelle du NRVD :



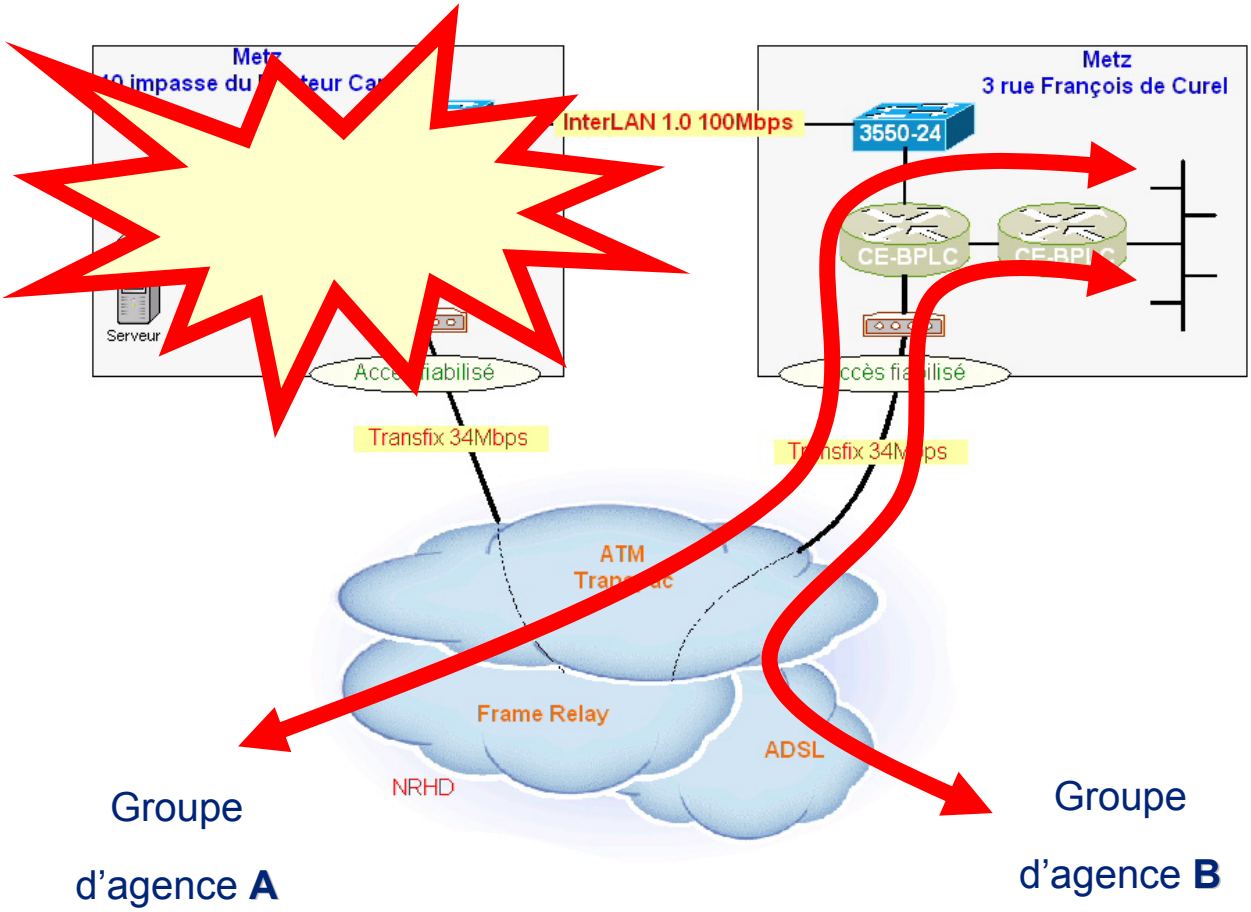
Quels sont les changements qui vont avoir lieu ?

En parallèle de l'optimisation du site central, est réalisée la fiabilisation de l'accès Internet. Comme je l'expliquerai dans la chapitre suivant, il s'agit de doubler les serveurs Internet afin d'avoir un site Internet de Back-Up. L'optimisation du site central consiste à relier le NRHD aux sites de Metz-Nord et de Metz-Centre, mais aussi d'avoir un interlan entre ces deux sites. Ce triangle permettra de passer en back-up à froid en cas de problème. Voici le schéma de l'évolution du NRHD :



Pour ne pas charger les lignes, les agences vont être divisées en deux groupes A et B. Ces deux groupes emprunteront des chemins différents pour atteindre les serveurs de productions qui se trouvent à Metz-Nord. Cela sera bien entendu transparent pour l'utilisateur puisque ces chemins seront paramétrés dans les routeurs. Cependant, en cas de problème sur une ligne (une pelleteuse maladroite par exemple) ou dans le cas d'un sinistre sur le site de production, toutes les agences seraient redirigées vers le site de back-up de Metz-Centre. C'est une opération manuelle qui sera réalisée par les responsables du centre informatique. En cas de problème, il est normalement possible de rétablir le service en deux heures de cette manière.

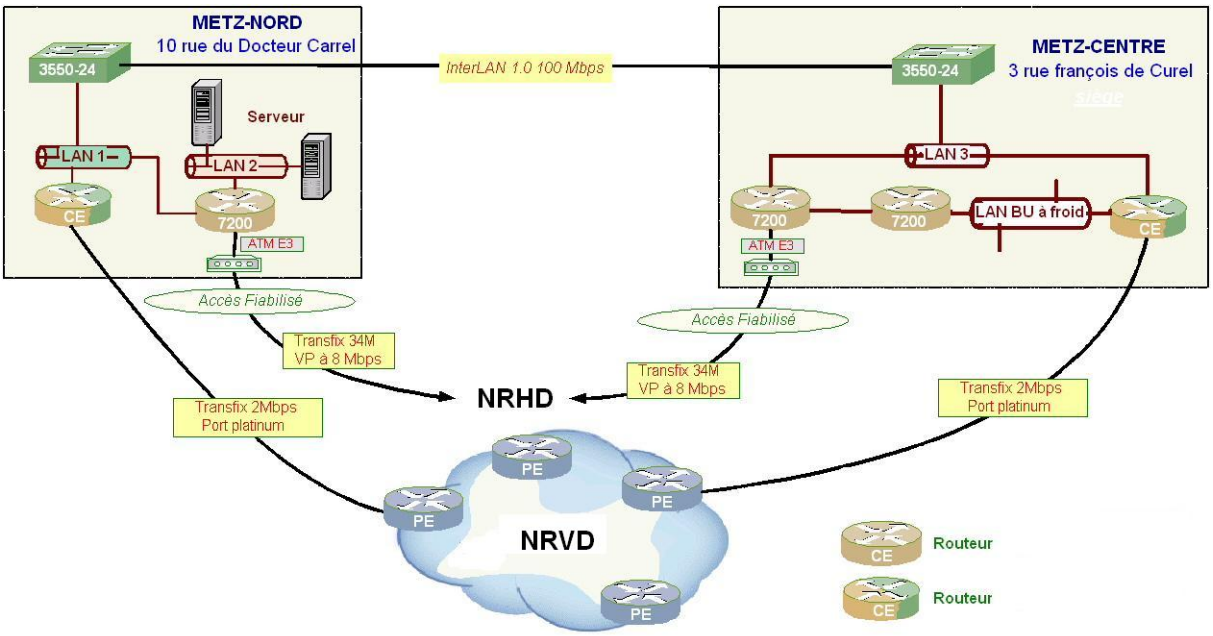
Voici le schéma du passage en back-up à froid :



En même temps que les améliorations apportées au NRHD, l'actuel réseau NRVD pilote est amené à être déployé. Trois nouvelles agences ont été reliées avant le début de l'été. L'objectif étant d'en relier une vingtaine voire plus sur 2005, une cinquantaine en 2006, puis bouclage des 130 agences en juin 2007.

Les agences du NRVD sont reliées au cœur de réseau en SDSL (ADSL à débit symétrique). Avant chaque basculement, il faut dimensionner les flux de chaque agence afin de lui attribuer un nombre de canaux adapté à ses besoins (sachant que permettre 13 communications simultanées correspond à une agence de50 à 60 employés).

Voici l'implémentation du NRVD :



Comme vous avez pu le constater sur le schéma en annexe I, le NRVD expérimental n'était relié qu'au site de production de Metz-Nord. A l'heure de la rédaction de ce rapport, France Télécom vient de relier le NRVD également à Metz-Centre.

Familiarisation avec Cisco :

Avec ses routeurs, commutateurs, réseaux d'accès et logiciels réseau, Cisco s'impose comme le leader mondial des solutions réseau pour Internet: plus de 50% de toutes les autoroutes de l'information utilisent du matériel Cisco, alors que plus de 80% de la technologie de base d'Internet émanent des laboratoires de recherche et développement de l'entreprise californienne.

Les produits Cisco sont des produits complexes offrant des possibilités très larges dans l'exploitation de réseaux. A l'heure actuelle, tous les équipements de la BPLC ont été au fur et à mesure remplacés par du matériel Cisco, notamment pour les possibilités que ce matériel offre au niveau QoS (Quality of Service).

Voici les principales fonctionnalités de la QoS Cisco : débit garanti, services différenciés, transmission accélérée, services intégrés, détection rapide et aléatoire, ressource reservation protocol (RSVP), mise en file d'attente pondérée, détection rapide et aléatoire pondérée.

Dès le début de mon stage, M. Forêt a souhaité que je me familiarise avec ce matériel. C'est pourquoi dès la première semaine, je me suis rendue sur le site de Metz-Nord avec lui pour remplacer un switch HP par un switch Cisco.

Le matériel CISCO étant entièrement configurable, il existe alors un langage de programmation spécifique à Cisco. M. Forêt s'occupant de l'aspect routage du réseau (entre autre) dispose d'une console à partir de laquelle il supervise tous les routeurs du réseau en telnet. Le protocole telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).

Le switch que nous allions remplacer était relié aux deux routeurs Cisco A et B, à deux gateway (interfaces entre téléphonie IP et Réseau téléphonique commuté), un IP phone, le routeur de France Télécom pour le NRVD. Avant toute chose, il fallait entrer une adresse IP dans la configuration du routeur. Nous avons ensuite débranché l'ancien routeur et installé le nouveau. Les diodes d'activité se sont correctement allumées et nous avons vérifié que l'IP phone fonctionnait correctement. Normalement, l'opération devait s'arrêter là, tout semblait fonctionner. Malheureusement, les agences en IP ont connu des incidents consécutivement à cette modification : pour certaines plus rien ne marchait, pour d'autres seulement certains services fonctionnaient. Après des heures de recherche en commun (l'équipe s'est mobilisée), nous avons trouvé que l'erreur provenait du routage. M. Forêt a donc modifié la table de routage et tout les service a été rétabli dans les agences en IP.

Suite à cela, on m'a prêté un switch Cisco qu'on s'apprêtait à installer ainsi qu'une console, afin que je me familiarise avec le langage Cisco. Toutes les erreurs étaient permises puisqu'il est possible de faire un reset complet du matériel. Je comprends enfin la raison pour laquelle Cisco dispense de nombreuses formations (très courues) sur ses produits, car leur configuration n'est pas instinctive… pour l'instant !

Malheureusement, nous étions repartis de Metz-Nord sans noter les ports sur lesquels nous avions reliés le matériel. Or il est important d'avoir des plans à jour décrivant ce qui est branché et où. Ainsi, en cas de problème, on peut faire intervenir un pupitreur présent sur place en lui décrivant le matériel. Cela a été une occasion rêvée pour me faire tester mes compétences Cisco. Mon rôle a été de retrouver à distance sur quels ports était branché le matériel. Or il n'existe pas de commande Cisco le permettant.

Les commandes qui m'ont été nécessaires sont :

```
Switch> sh ip arp vlan 1
```

Cette commande permet d'afficher l'adresse IP et la MAC adresse du matériel. Normalement, d'après l'adresse IP, on sait de quoi il s'agit.

```
Switch> sh mac-address-table interface fastEthernet 0/1
```

Cette commande permet d'afficher la MAC adresse du matériel branché sur le port sélectionné.

Attention, pour que ces commandes soient exploitables, il faut que la table arp soit « fraîche » ; on doit donc faire un ping du broadcast depuis un PC juste avant de les taper.

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle *Protocole de résolution d'adresse* (en anglais ARP signifie *Address Resolution Protocol*).

D'autre part, par la suite, on a fait appel à mon esprit néophyte pour proposer une nouvelle configuration des routeurs du réseau. Peut être étais-je en mesure de trouver une solution à laquelle personne n'aurait pensé. A l'heure actuelle les routeurs utilisés par la BPLC sont les suivants :

- Cisco 7200 pour le site central,
- Cisco 2611/2611XM/2621XM pour les agences,
- Cisco 805 pour les G.A.B,
- Cisco 2651 pour le NRVD.

Les routeurs qui sont à la source des interrogations, sont les gros routeurs 7200. Ils sont actuellement agencés de la même manière que sur le plan en annexe I. Je me suis donc armée de tous les outils de recherche possible : documentation Cisco, Internet, logiciel de configuration.

Etant néophyte, le logiciel de configuration s'est avéré compliqué, car il nécessite à la base une bonne connaissance des produits Cisco. Heureusement, le site Internet de Cisco présente leur gamme et les possibilités du matériel.

Recherche :

Ma réflexion m'a amenée à deux conclusions majeures concernant l'architecture du réseau :

⇨ Les gros routeurs Cisco 720(4) et 720(6) (4, pour 4 emplacements-cartes et 6, pour 6 emplacements-cartes) sont souvent sous exploités, c'est-à-dire que tous slots ne sont pas utilisés. On pourrait dans ce cas envisager de les remplacer par des modèles de gamme inférieure. Cependant, cela est rendu impossible puisque ces routeurs sont reliés au Host par des liaisons de type « Channel », c'est un gros câble contenant une fibre optique. D'autre part ces routeurs sont utiles car ils combinent cartes série et cartes ATM. Ils ne seront donc pas remplacés.

⇨ Sur le site de Metz-Centre, il y a actuellement deux routeurs Cisco 7200 pour les Cisco B et E. Ceux-ci pourraient être remplacés par un seul. En effet, sur le Cisco B, il y a beaucoup de liaisons série qui ne fonctionnent plus, on peut éventuellement envisager de retirer une carte série pour y mettre une carte ATM, le Cisco B serait ainsi relié directement au NRHD. Malheureusement, des subtilités de configuration Cisco empêchent cette manipulation. Il est donc nécessaire de conserver le routeur Cisco E. Le routeur Cisco n'étant utilisé que pour le raccordement en ATM du NRHD au réseau, on peut prévoir l'extinction future du NRHD, ainsi ce routeur ne servira plus.

⇨ Actuellement, les G.A.B. de test de Metz-Centre sont sur un sous-réseau isolé. Ce sous-réseau, n'est plus désirable actuellement. Ces G.A.B. seront désormais directement sur le réseau. Le switch de ce sous-réseau est actuellement un HP, il serait profitable de le remplacer par un Cisco, ce qui permettrait de faire de la QoS.

⇨ Il serait peut-être nécessaire de créer un second réseau à Metz-Centre pour le NRVD. Cela ferait une infrastructure de secours ou de partage de charge.

⇨ Question importante : sur quels routeurs implanter la liaison interlan 100 Mbits/s ? A priori, j'ai proposé Cisco E et Cisco A, c'étaient effectivement ceux qui me paraissaient prédestinés à cela. Après une réunion avec les ingénieurs de chez France Télécom/Transpac/Equant, il a été convenu de raccorder cet interlan à deux switchs/routeurs eux-mêmes reliés au réseau et aux routeurs du NRVD.

⇨ Un autre switch de Metz-Nord doit être changé pour passer en Cisco. Ce switch supporte en majorité les serveurs de messagerie Notes. Je me suis rendue sur place avec M. Ihout, responsable Notes. Nous avons repéré les emplacements, et quels allaient être les serveurs Notes supprimés afin de connaître la capacité du switch dont nous avons besoin. Nous installerons ce switch dans quelques jours.

Tous ces points ont été traités lors d'une réunion du 18 mai, en présence de M. Forêt, des responsables Internet ainsi que France Télécom/Transpac/Equant. En a résulté un schéma

récapitulatif que vous trouverez en fin de rapport, car il contient également les conclusions de la partie Internet.

5 - Fiabilisation de l'accès Internet

Dans le cadre de la refonte de son réseau, la BPLC souhaite fiabiliser son accès Internet par le biais d'un site Internet de back-up. Après avoir défini clairement la raison d'être du back-up, il s'agit alors de délimiter les besoins : quels sont les serveurs vitaux à dupliquer ? Sur quels critères mettre en place ce back-up ? Cela nécessite une connaissance de l'infrastructure existante ainsi que des possibilités de duplication des serveurs. Cette opération sera mise en place après l'installation de lignes interlan France Telecom prévue fin mai 2005.

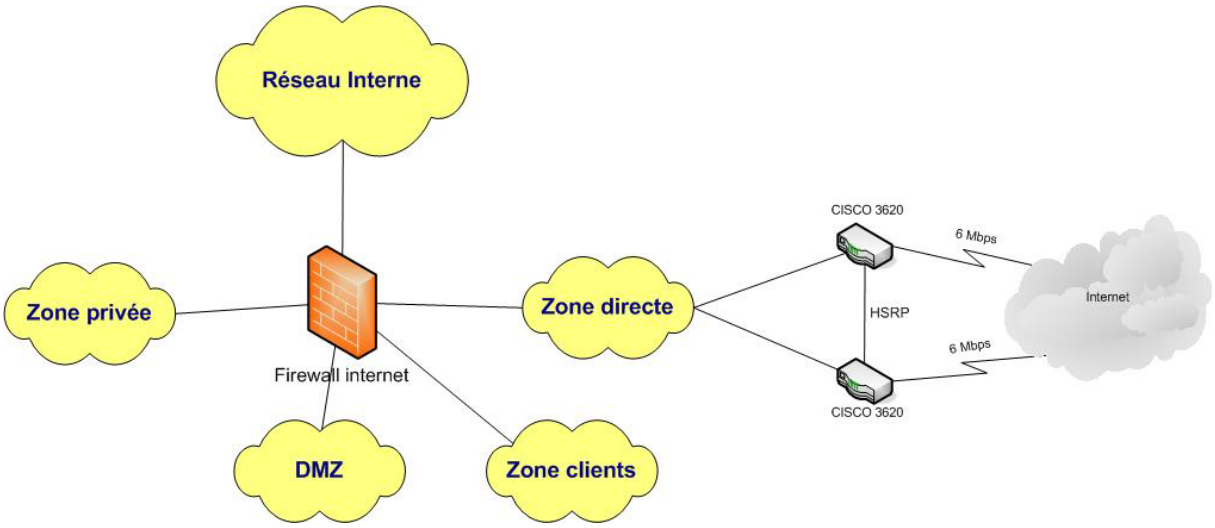
Raison d'être du back-up :

A l'heure actuelle, en cas de problème (incendie, dégât des eaux,…) sur les machines Internet, la solution de secours consiste à utiliser les cassettes de sauvegardes effectuées régulièrement. Dans ce cas de figure, il faut mettre en service de nouvelles machines, installer les applications nécessaires, et les mettre à jour à l'aide des sauvegardes. Il s'agit d'une solution laborieuse et nécessitant du temps, qui peut être améliorée, afin de préserver la continuité du service et de perdre un minimum de temps en situation d'urgence.

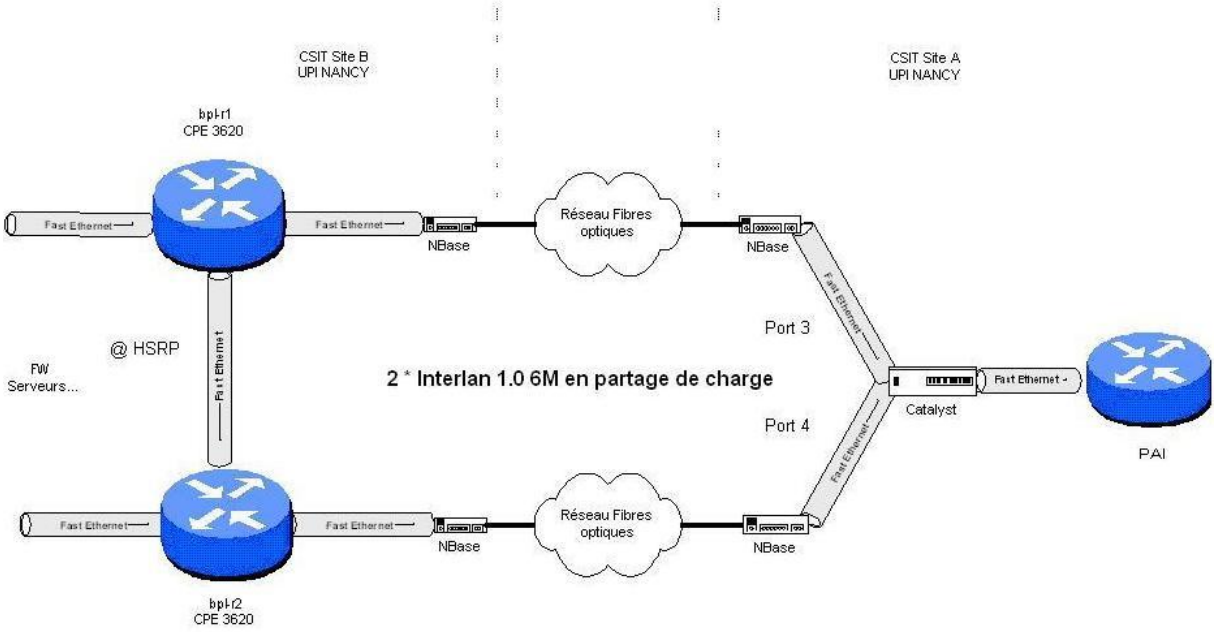
La solution d'un site Internet de back-up s'avère être particulièrement adaptée au problème que nous abordons. En effet, puisque la BPLC dispose de deux sites géographiquement distincts à Metz-Centre (Curel) et à Metz-Nord (Carrel), autant s'en servir pour éloigner et doubler des serveurs importants. La probabilité d'un incident sur les deux sites en même temps étant moindre, cette solution offre la possibilité d'une continuité des services assurés par les serveurs.

Infrastructure existante :

Le réseau informatique de la BPLC, comprend une zone Internet divisée en plusieurs zones : direct, privé, clients. Chaque zone comprend des machines : la zone directe comprend les machines de clients situées avant le firewall, la zone client (+ serveurs mutualisés) comprend des machines clients situées derrière le firewall, et enfin, la zone privée comprend les serveurs de la BPLC, ceux-ci hébergent des applications indispensables aux opérations et services bancaires.



Actuellement, Internet arrive sur deux routeurs CISCO 3620 (fonctionnant en secours et partage de charge) par le biais de liaisons 6 Mbps. En fait, ces routeurs ne sont vus que sous une seule adresse IP par le réseau. Outre la zone Internet directe, les autres zones sont derrière le firewall Internet.

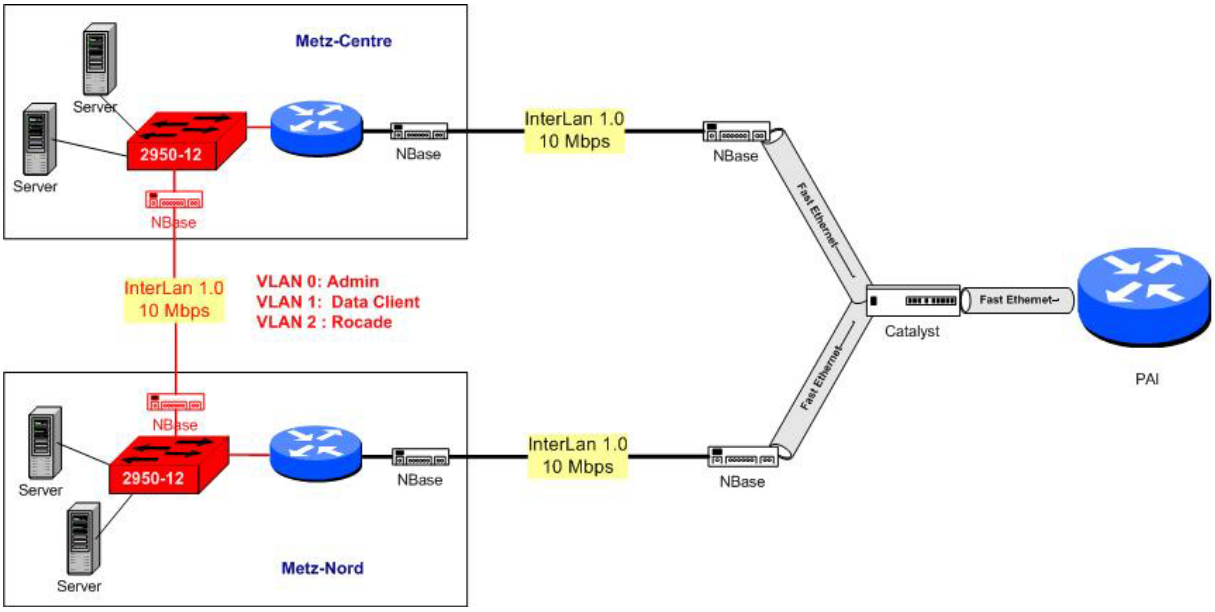


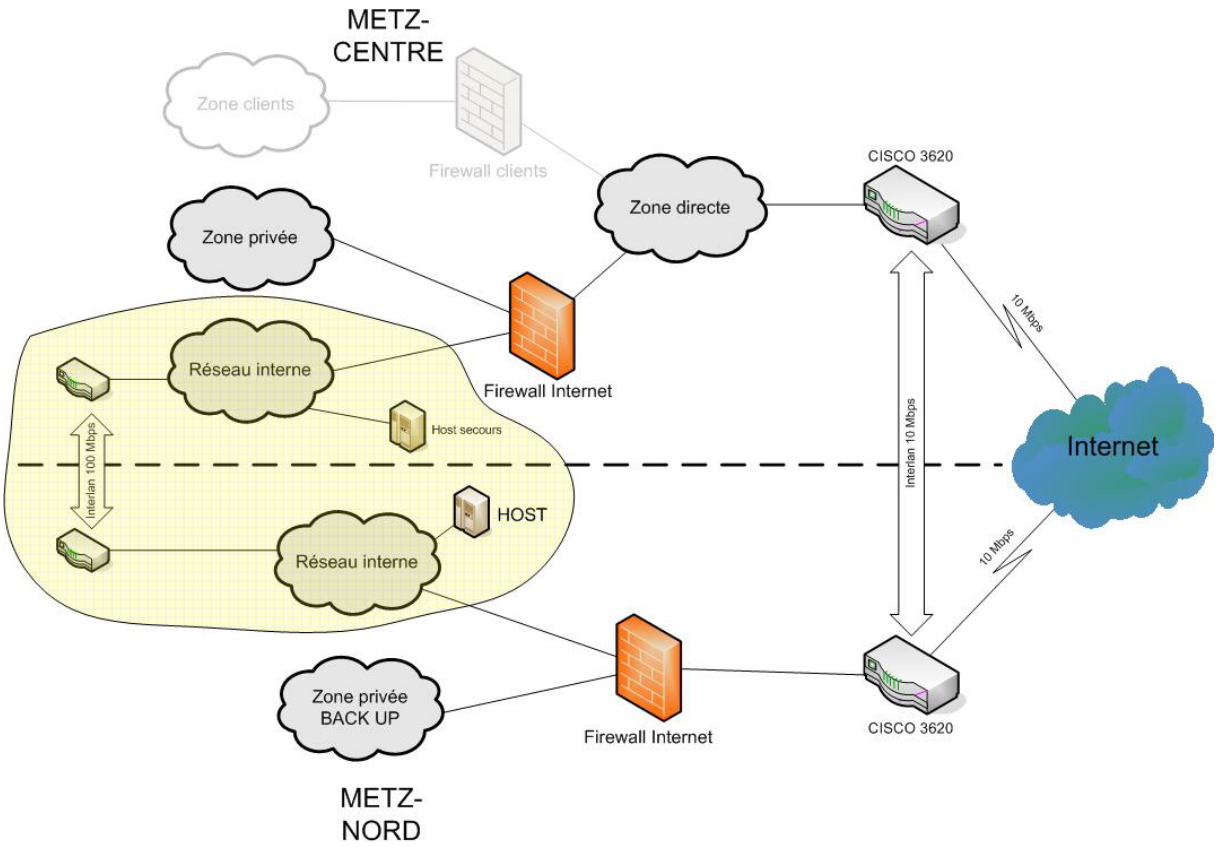
La mise en place du back-up Internet va se décomposer en deux parties : la création d'une nouvelle architecture de la partie Internet et la duplication de certains serveurs pour le back-up.

Nouvelle architecture :

Le but de mon stage est de proposer une nouvelle architecture pour le déploiement de la zone de back-up. Il va donc me falloir tenir compte des exigences imposées par la sécurité, qui m'ont été fournies.

Tout d'abord, les deux lignes d'accès Internet vont passer de 6 Mbps à 10 Mbps. Il va également falloir déplacer un des deux routeurs 3620 vers le site de Metz-Nord, ainsi qu'une des deux arrivées Internet. D'autre part, la BPLC souhaite séparer les flux « client » et les flux « privé » en les faisant traiter par des firewalls différents. Les deux sites seront reliés par un interlan 10 Mbps.





Serveurs Internet :

Les serveurs qui sont concernés sont les serveurs de la partie privée. Il s'agit de serveurs utilisés pour des applications bancaires en lignes (banque en ligne, commerce électronique, services sms…), des applications de messagerie ainsi que les serveurs de DNS.

Il s'agit de déterminer quels serveurs sont vitaux et nécessitent un back-up régulier. Pour cela, il faut bien cerner leurs applications et leur finalité. Cette étude doit être menée en parallèle avec le service des études qui développe les applications serveurs.

⇨ **E-bank**, serveur de banque en ligne, est le serveur le plus compliqué.
- Envoi de mails avec certificats aux clients.
- Interface entre le client et le host, toutefois certaines informations stockées en local sur la machine pour éviter d'aller consulter en permanence le host.
- Base des virements : virements effectués immédiatement + sauvegarde des virements différés. A prendre en compte dans le back up ! (traitement tous les matins à 6h30).
- Base interrogeable par allodis (connaissance de tous les mouvements du client jusqu'à la veille incluse).

⇨ **E-com**, serveur de commerce électronique.
- Divisé en 2 parties.
- D'une part, des données qui ne sont pas sur le host (back-up du jour et données non vitales pour le client)

- D'autre part, l'interface de paiement.
- Bases de test : pas de nécessité de back-up.
- Base des activités e-commerce ouverte en FTP.
- Envoi de mails.
- Possibilité d'établir précisément ce qui doit être back-upé.

⇨ **Vitrine :** serveur support de la vitrine, sauvegarde facile. Indispensable vis-à-vis de la clientèle, permet d'accéder à la banque en ligne.

⇨ **SMS+ :** nouveau service permettant la réception de sms sur demande à un numéro surtaxé.
- Services opérés par une société (simple interrogation du host pour connaître les infos des comptes bancaires).
- Serveur simple à dupliquer.

⇨ **Moviplus :** service avec abonnement qui envoie régulièrement des sms aux clients pour les tenir informés de l'état de leurs comptes.
- Serveur simple à être dupliqué.

⇨ **Serveur DNS :** attribution des noms de domaine aux adresses IP (correspondance adresse virtuelle/ adresse physique)
- sauvegarde permanente, réplication.
- Une troisième machine aurait déjà les infos.

⇨ **Comweb :** gestion de documents.
- Données statiques : facile à dupliquer.

⇨ **MESSA :** quelques problèmes restent à résoudre.

⇨ **Certificats :** peu utilisé pour l'instant.
- génération de certificats à la demande (par un programme)
- à priori, simple sauvegarde nécessaire.

Il faut trouver une solution adaptée à tous les serveurs ainsi qu'à chaque serveur en particulier. Des réunions ont eu lieu afin de décider ensemble des serveurs à copier et des priorités. On pourra éventuellement faire passer plusieurs serveurs sur la même machine, s'ils sont compatibles, quitte à en faire fonctionner certains en mode dégradé.

Possibilités de duplication et mises à jour :

Une fois qu'une conformation exploitable aura été trouvée pour le back up, il s'agira de mettre en place des sauvegardes régulières de chaque serveur afin d'être en possession de serveurs à jour lors du back-up à froid. Il s'agit de trouver une solution physique et logicielle pour réaliser cette sauvegarde.

D'un point de vue physique, il s'agit d'établir un lien de communication entre les deux sites de Metz-Centre et de Metz-Nord. Pour ce faire il existe deux interfaces : l'interlan 10 Mbps et l'interlan 100 Mbps. Le premier serait idéal dans la mesure où il relie directement les

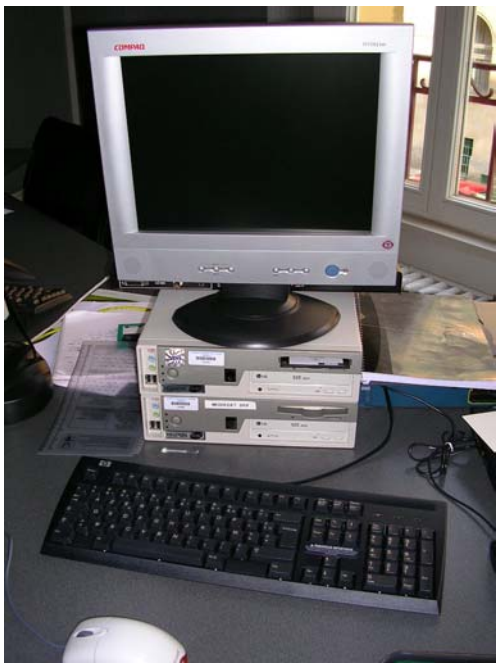
sites Internet entre eux, mais il est limité par un débit insuffisant, le second, d'un débit confortable, permettrait l'échange de flux de manière acceptable. Seul bémol : les flux Internet et bancaire seraient mélangés. Malgré cela, cette solution me paraît la meilleure puisque ces deux types de flux restent des flux privés, auxquels seuls les postes privés ont accès. C'est finalement cette solution qui a été choisie.

D'un point de vue logiciel, un large panorama de solutions s'ouvre à nous. Il faudra déterminer en équipe quel logiciel s'avère être le meilleur. A ce jour nous avons 6 logiciels à comparer : Double Take, Mirror Folders, BackUp Exec, Symantec Livestate Recovery, ainsi que deux sharewares. Leurs possibilités doivent être évaluées en fonction des besoins.

Tests des logiciels :

Pour la mise en place du site de back up, l'utilisation d'un logiciel de réplication s'avère être indispensable pour maintenir les serveurs de back up à jour. Quels que soient les critères de réplication imposés par les serveurs et les applications qu'ils contiennent, il s'agit de trouver un logiciel efficace, simple et dimensionné pour ce que l'on veut en faire. Après quelques recherches en équipe, nous avons retenu quelques logiciels susceptibles de convenir pour nos opérations. Nous les avons donc testés.

Protocole : nous avons installé deux machines en réseau de manière à recréer la configuration de machine-source et de machine-cible pour la réplication. Nous leur avons attribué une adresse IP. Si besoin, une tierce machine peut servir de console de management.



Double Take 4.4 (édité par Sunbelt Software)
http://www.sunbelt-software.com/Double-Take.cfm

Double Take est un logiciel de réplication de données pour des serveurs en environnement Microsoft. Sa description le rend particulièrement intéressant dans notre situation. Le site de son éditeur propose une version d'évaluation, pour télécharger cette dernière, il faut rentrer ses coordonnées, on est par la suite assez rapidement contacté par un ingénieur-commercial. Pratique si on rencontre quelques difficultés lors du test se dit-on !

Le logiciel propose deux versions : la version serveur + client et la version client, le choix se fait à l'installation. Il conviendra d'installer la version serveur + client sur les serveurs et la version client sur un poste qui ne servira qu'à superviser les opérations. L'installation est relativement facile puisque les ordinateurs du réseau ayant Double Take se détectent automatiquement. Attention toutefois, les droits d'administration ne sont pas attribués automatiquement sur la version serveur, il convient donc d'effectuer la manipulation à la main.

Une fois le logiciel installé, il faut paramétrer les tâches que l'on veut lui faire exécuter. Le manuel d'utilisation (en anglais) est assez dense (398 pages) mais il fait le tour de toutes les possibilités que propose le logiciel, et il explique la façon dont il procède. On découvre ainsi que les opérations peuvent être supervisée par une interface graphique ou en mode texte. Nous avons effectué le test en mode graphique.

Ce logiciel permet diverses opérations :
- le « mirroring » : copie exacte de données vers une cible,
- la réplication : transmission en temps réel de changements apparus dans des fichiers sélectionnés,
- le « failover » : processus qui permet à une machine cible de prendre la place d'une machine source dans le cas ou celle-ci tomberait.
- on peut également faire une restauration de serveur.

Lors du test du logiciel, j'ai effectué les tests des différentes possibilités les unes après les autres, en suivant les instructions du mode d'emploi. Ce qui nous intéresse, dans notre configuration, est plutôt la réplication en temps réel des données qui sont sur les serveurs. La création d'un « replication set » est très simple, il suffit de choisir un serveur-source et un serveur-cible ainsi que les fichiers à répliquer et l'endroit où ils doivent l'être. Lors de la première exécution, un « mirroring » s'effectue puis, par la suite, le logiciel ne tient plus compte que des changements des fichiers. Bien entendu, on peut affiner la configuration du « replication set » en limitant la bande passante utilisée, le début, la durée, la fin, la fréquence des réplications. Ce procédé fonctionne très bien et laisse entrevoir la possibilité de différentes configurations de réplication des données.

Toutefois, la procédure de failover s'avère être facile à mettre en œuvre mais malgré une lecture scrupuleuse de la notice d'utilisation et plusieurs essais, la procédure de retour à la normale est difficile. Après un contact avec le support de Sunbelt Software, personne n'a été en mesure de m'aider, j'attends d'ailleurs encore qu'on me rappelle. De toute façon, il apparaît que cette fonctionnalité n'était pas intéressante pour ce qu'on cherche à faire, l'équipe informatique souhaitant faire une procédure manuelle, bien plus fiable !

Enfin, critère de choix important, ce logiciel coûte 2 495 € par machine. Ce qui le rend beaucoup moins accessible, quelle que soit la configuration qu'on choisira pour la réplication (en raison du nombre élevé de serveurs).

Symantec LiveState Recovery Standard Server(édité par Symantec)
http://sea.symantec.com/content/product.cfm?productid=24

Logiciel très séduisant sur son site Internet, LiveState Recovery permet de faire toutes sortes de sauvegardes et back-ups. Le site propose une version d'évaluation, on peut donc tester le produit pendant 30 jours.

Comme pour Double Take, on peut installer une version « Agent » destinée aux serveurs et une version « Console » destinée au management des tâches. L'installation, est plus aisée qu'avec le précédent logiciel. J'ai installé deux versions « Agent » sur mes deux serveurs ainsi qu'une version « Console » sur mon poste afin d'administrer l'ensemble. Malheureusement, lors de la configuration du dispositif : surprise aucun des deux serveurs n'apparaît sur la console… après réflexion, on a pu déterminer que ces ordinateurs ne sont pas sur le même domaine (au sens de Microsoft) et il est indiqué, seulement dans le mode d'emploi, que ce logiciel ne peut effectuer des opérations de sauvegarde que sur des serveurs du même domaine. Malheureusement, c'est un très mauvais point puisque, dans notre cas, les serveurs ne seraient pas tous dans le même domaine.

Malgré ce petit désagrément, il était intéressant de voir comment fonctionne ce logiciel. J'ai alors installé une version « Console » sur un des deux serveurs. C'est à cet instant qu'on constate que la notice d'utilisation n'est pas très détaillée. L'utilisation du logicielle n'est pas très intuitive et il est plutôt difficile de retrouver comment configurer toutes les possibilités présentées sur le site internet. Je conclus que ce logiciel est plutôt un outil de back up de partition pour stockage sur un autre support ou une autre machine, les fonctionnalités de réplication en temps réel n'apparaissant pas dans l'outil de configuration.

Après contact du service avant-vente (à noter : très aimables), j'ai bien eu confirmation que la version Standard Server n'offrait pas les possibilités recherchées.

Il me reste donc à tester la version Manager ou Advanced server que je devrai recevoir sur CD rapidement.

Symantec LiveState Recovery Adavanced Server(édité par Symantec)
http://sea.symantec.com/content/product.cfm?productid=24

La version Advanced Server est la version supérieure à la version Standard Server. C'est cette version que Symantec m'a fait parvenir. Comme pour la version Standard, il est encore impossible d'administrer les sauvegardes à partir de la console installée sur mon poste de bureau. Ce problème demeurant toutefois étrange, j'ai posé la question au support Symantec qui, à cette heure, ne m'a toujours pas répondu. Pour palier à ce problème, j'ai une nouvelle fois installé la version « console » sur un des deux serveurs. Là, il devient aisé de configurer une opération de sauvegarde entre mes deux serveurs de test. Notons, qu'il a fallu

faire une manipulation afin de configurer la connexion au réseau du service LiveState Recovery en allant dans la gestion de l'ordinateur et en choisissant un compte pour se connecter. Cette manipulation n'était pas indiquée dans le mode d'emploi et nous a donné du fil à retordre.

Il est donc maintenant possible de configurer une opération de sauvegarde entre mes deux serveurs de test. On a la possibilité de choisir entre des sauvegardes incrémentielles ou des sauvegardes complètes, mais au niveau de la planification, les options proposées sont relativement restreintes. Une sauvegarde s'effectue immédiatement après validation de l'opération, il y a possibilité de choisir la vitesse de l'opération, afin de ne pas encombrer le réseau.

Après quelques manipulations, il a été possible d'afficher les serveurs sur une console d'administration distante. Malheureusement, j'ai encore été confrontée à un problème : le logiciel arrivait à se connecter à un des deux serveurs sans problème, mais pas au second. Après vérifications, les deux machines ont exactement les mêmes paramètres de connexion, les identifiants et les mots de passe ont été vérifiés. Face à ce phénomène, nous avons réalisé une analyse des trames IP lorsque les ordinateurs se connectent entre eux, puis nous avons comparé les trames concernant la machine qui se connectait sans problème et celles de celle pour laquelle c'était impossible. Il s'avère que l'erreur apparaît lorsque la machine attribue un port pour la connexion. La trame indique « MSRPC fault ». A l'heure qu'il est nous n'avons pas trouvé comment régler ce problème, et le support technique ne souhaite plus nous aider puisque nous n'avons pas acheté le produit. A voir…

BackUp Exec (édité par Veritas)
http://www.veritas.com/Products/www?c=product&refId=57&ln=fr_FR

BackUp Exec est un logiciel de gestion de données sur des réseaux de serveurs Windows. Ce logiciel n'est pas adapté à nos besoins puisqu'il est conçu pour la sauvegarde sur bandes. Dommage car on pourra noter la présence d'un mode d'emploi très détaillé, ainsi que d'une interface complète.

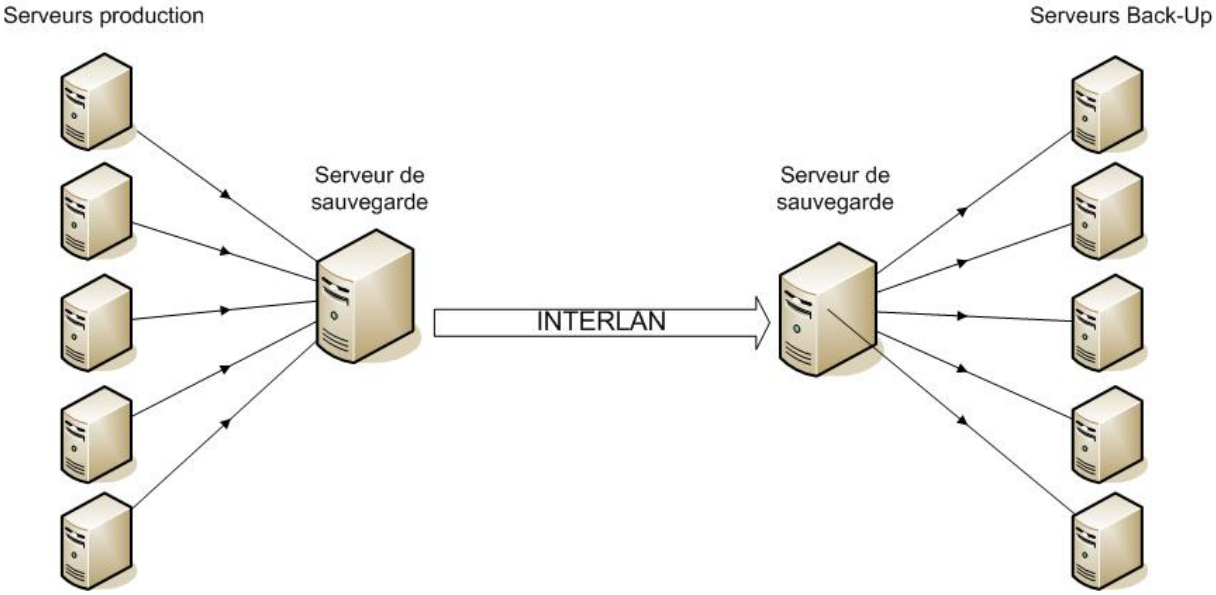
Mirror Folder (édité par Techsoft)
http://www.techsoftpl.com/backup/index.htm

Mirror Folder est un logiciel de réplication en temps réel sur n'importe quel support appartenant au réseau, à partir du disque dur local. Il permet de configurer quelques options de duplication. En outre, son interface est entièrement intégrée à Windows. La réplication de répertoire d'une machine à l'autre est simple, puis la modification de fichiers en temps réel fonctionne. Les opérations de synchronisation peuvent être planifiées, cependant on ne peut pas paramétrer d'autres options comme le pourcentage d'utilisation de la bande passante. Toutefois, on notera que lorsqu'un fichier est répliqué vers un répertoire, il devient impossible de le répliquer vers un autre répertoire, les options devenant grisées. On remarquera que ce produit a montré ses faiblesses au cours des divers tests : des bugs, induisant des problèmes de fiabilité.

Enfin, ce produit fonctionne uniquement dans un environnement Windows sur des réseaux Windows. Cela pourrait poser des problèmes d'ouverture de ports spécifiques au réseau windows.

Evolution du projet :

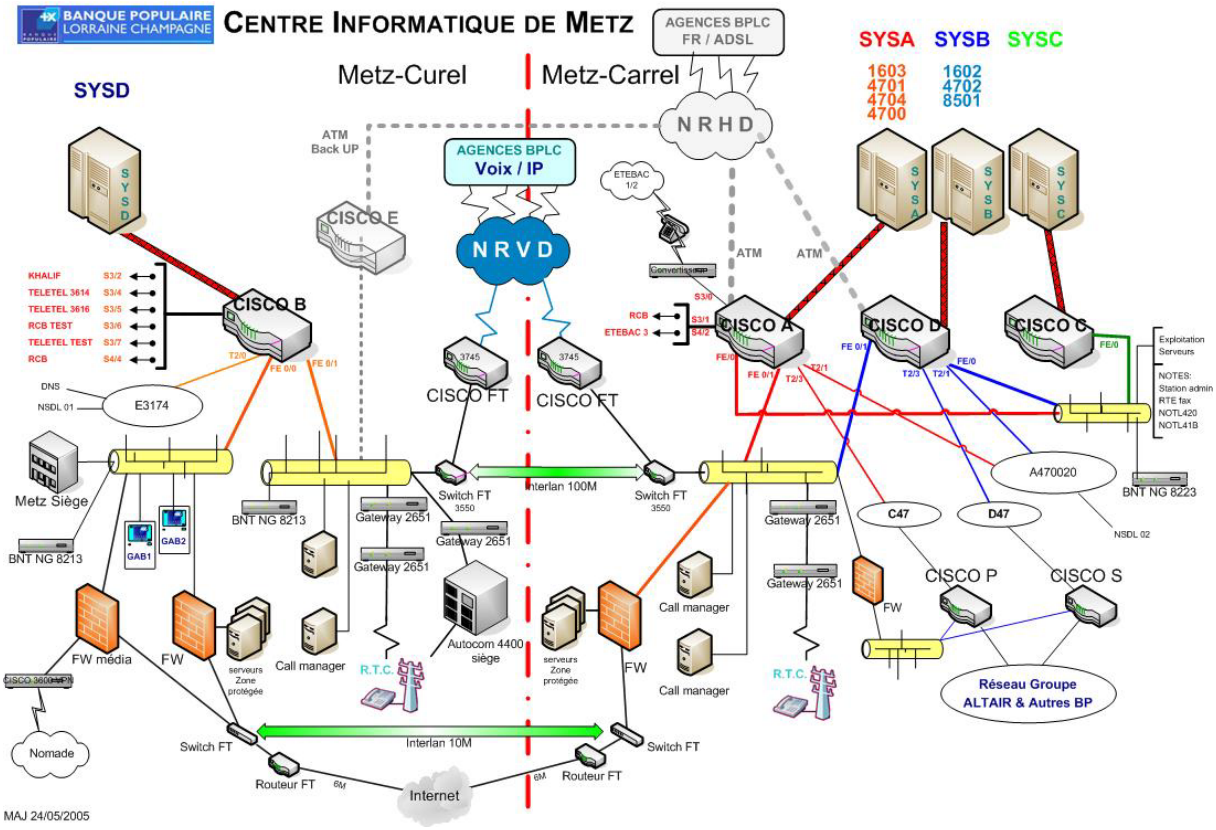
A l'heure actuelle, le projet Internet est toujours en cours de déploiement, une décision a été prise concernant le mode de réplication des serveurs. Il s'agira donc de mettre un serveur de réplication centralisée de chaque côté de l'interlan. Comme sur le schéma suivant :



Il nous reste encore à examiner la possibilité de répliquer les données par simple protocole FTP ou à l'aide d'une solution RAID. Malheureusement, les lignes interlan France Télécom sont en attente depuis début Avril, nous n'attendons qu'elles pour pouvoir commander et installer les serveurs de back-up sur le site de Metz-Nord. Sur le plan technique, une liste de pannes a déjà été prévue, avec un listing de solutions proposées par France Télécom dans chaque cas précis. Les actions conjointes de la BPLC et de France Télécom seront alors plus efficaces en cas de pannes.

Synthèse :

L'aboutissement des réflexions sur l'optimisation du site central et la fiabilisation de l'accès Internet développés dans les chapitres précédents ont permis de réaliser un nouveau schéma global du réseau.



Conclusion

L'étude des besoins, l'analyse du projet et sa réalisation en équipe m'ont permis de prendre part à un projet riche et intéressant dans le domaine des réseaux et de la prévention de sinistre. J'ai ainsi pu approfondir un domaine que j'ai abordé très superficiellement lors de mon cursus en MST Télécoms.

L'aspect recherche personnelle a été primordial pour la phase d'étude de l'existant et la mise au point de propositions concrètes. Même si on se sent perdu au départ, il est satisfaisant de se rendre compte que l'on avance malgré tout.

D'autre part, j'ai pu prendre part à la vie d'un service informatique et de son équipe, qui m'ont réservé un accueil chaleureux et ont contribué à une ambiance de travail conviviale. Je pense m'être bien intégrée au sein de l'équipe. Sur ce point, c'est l'aspect humain du stage qui se trouve grandi.

A l'heure actuelle, le projet de refonte du réseau est encore en cours et l'implémentation du site de back-up Internet n'a pas encore débuté. C'est pourquoi je vais prolonger cette expérience durant l'été à la Banque Populaire Lorraine-Champagne.

En conclusion, ce stage a été une expérience enrichissante tant sur le plan technique qu'humain et m'a permis de découvrir un domaine méconnu et d'envisager une poursuite d'études dans ce domaine.

Annexes

Annexe I : plan du réseau avant modifications

Annexe II : plan d'Internet avant modifications

Annexe III : plan d'Internet après modifications

Annexe IV : nouveau plan du réseau